arXiv:1304.7745v1 [cs.IT] 29 Apr 2013

On the Capacity of the Finite Field Counterparts of Wireless Interference Networks

Sundar R. Krishnamurthy and Syed A. Jafar

Abstract

This work explores how degrees of freedom (DoF) results from wireless networks can be translated into capacity results for their finite field counterparts that arise in network coding applications. The main insight is that scalar (SISO) finite field channels over $\mathbb{F}_{p^n}$ are analogous to $n \times n$ vector (MIMO) channels in the wireless setting, but with an important distinction – there is additional structure due to finite field arithmetic which enforces commutativity of matrix multiplication and limits the channel *diversity* to n, making these channels similar to diagonal channels in the wireless setting. Within the limits imposed by the channel structure, the DoF optimal precoding solutions for wireless networks can be translated into capacity optimal solutions for their finite field counterparts. This is shown through the study of the 2-user X channel and the 3-user interference channel. Besides bringing the insights from wireless networks into network coding applications, the study of finite field networks over $\mathbb{F}_{p^n}$ also touches upon important open problems in wireless networks (finite SNR, finite diversity scenarios) through interesting parallels between p and SNR, and n and diversity.

1 Introduction

Precoding based network alignment (PBNA) is a network communication paradigm inspired by linear network coding and interference alignment principles [1–3]. While intermediate nodes only perform arbitrary linear network coding operations which transform the network into a one-hop linear finite field network, all the intelligence resides at the source and destination nodes where information theoretically optimal encoding (precoding) and decoding is performed to achieve the capacity of the resulting linear network. The two restricting assumptions — restricting the intelligence to the source and destination nodes, and restricting to linear operations at intermediate nodes — are motivated by the reduced complexity of network optimization and also by the potential to apply the insights and techniques developed for one-hop wireless networks. Indeed, the PBNA paradigm gives rise to settings that are analogous to 1-hop wireless networks, albeit over finite fields. To highlight this distinction, we simply refer to these networks as finite field networks. There is a finite field counterpart to every 1-hop wireless network and vice versa. A number of interesting interference alignment techniques have been developed for 1-hop wireless networks and shown to be optimal from a degrees of freedom (DoF) perspective. Translating the DoF optimal schemes for wireless networks into capacity optimal schemes for finite field networks is therefore

Sundar R. Krishnamurthy (email: srkrishn@uci.edu) and Syed A. Jafar (email: syed@uci.edu) are with the Center of Pervasive Communications and Computing (CPCC) in the Department of Electrical Engineering and Computer Science (EECS) at the University of California Irvine. This work is accepted for presentation in part at ISIT 2013.

a promising research avenue. For example, the CJ scheme originally conceived for the K user *time-varying* wireless interference channel in [4] is applied to the 3 unicast problem by Das et al. in [1–3]. While the CJ scheme has also been applied successfully to the constant channel setting in wireless networks by using the rational dimensions framework of Motahari et al. in [8], the constant channel setting remains much less understood. In this work, we study constant channel settings, but over the finite field $\mathbb{F}_{p^n}$.

The main contributions of this work are general insights into the correspondence between degrees of freedom of wireless networks and capacity results for their finite field counterparts. In the wireless setting, constant scalar (SISO) channels are challenging because they lack the diversity needed for linear interference alignment schemes. Constant finite-field channels over $\mathbb{F}_{p^n}$ however, can be naturally treated as non-trivial $n \times n$ MIMO channels. A single link over $\mathbb{F}_{p^n}$ has capacity $n \log(p)$, similar to n channels of capacity $\log(p)$ each. There is an immediate analogy to n parallel wireless channels which would have a first order capacity $\approx n \log(\text{SNR})$, establishing a correspondence between n and "diversity" (number of parallel channels) and between p and SNR. Indeed, while scalar channels in $\mathbb{F}_{p^n}$ can be treated as $n \times n$ MIMO channels over the base field $\mathbb{F}_p$, these channels exist in a space with diversity limited to n, i.e., any $n+1$ of these $n \times n$ channel matrices are linearly dependent over $\mathbb{F}_p$. Also, because of their special structure these channel matrices satisfy the commutative property of multiplication (inherited from the commutative property of multiplication in $\mathbb{F}_{p^n}$). Contrast this with generic $n \times n$ MIMO channels in $\mathbb{F}_p$, which occupy a space of diversity n^2 and generally do not commute. The difference is consistent with the interpretation of $\mathbb{F}_{p^n}$ channels as similar to diagonal channels which have diversity only n, and are also commutative. These insights are affirmed by translating the DoF results from fixed diversity wireless networks to their $\mathbb{F}_{p^n}$ counterparts. Especially in the 3 user interference channel, the role of n as the channel diversity becomes clear.

Other interesting aspects of this work are finer insights into linear interference alignment and the techniques used to prove resolvability of desired signals from interference. Whereas in wireless networks, linear interference alignment is feasible for either almost all channel realizations or almost none of them and is relevant primarily to the slope of the capacity curve in the infinite SNR (DoF) limit, in the finite field setting the fraction of channels where linear alignment is feasible can be a non-trivial function of p, so that not only we have the $p \to \infty$ behavior which corresponds to the wireless DoF results, but also we have an explicit dependence of linear alignment feasibility on p for finite values of p. By analogy to finite SNR, this is intriguing for its potential implications, even if the analogy is admittedly tenuous at this point. Since these finer insights are a priority in this work, we will not rely only on $p \to \infty$ assumptions to establish the capacity of the finite field networks. Instead, our goal will be to identify the capacity for all p as much as possible. Because of this focus on constant channels and finite p, the linear independence arguments required to show resolvability of desired and interfering signals, become a bit more challenging for finite p, and require a different, somewhat novel approach. Finally, while we focus primarily on the X channel and 3 user interference channel to reveal the key insights, the insights seem to be broadly applicable and sufficient for extensions beyond these settings.

We begin with the X channel.

2 X Channel

An X network is an all-unicast setting, i.e., there is an independent message from each source node to each destination node. In this work we study an X network with 2 source nodes, 2 destination nodes, and 4 independent messages as illustrated in Fig. 1, also known simply as the X channel.

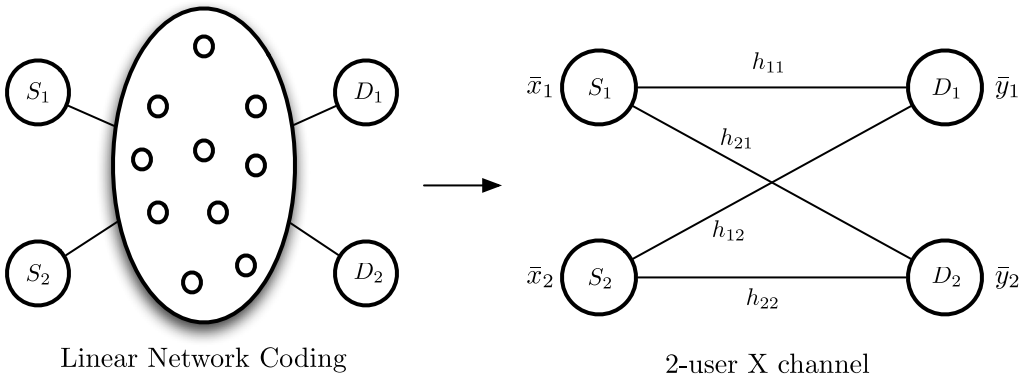

Figure 1: Wired network modeled as 2-user X channel

2.1 Prior Work

The X channel, which contains broadcast, multiple access and interference channels as special cases, is one of the simplest, and also one of the earliest settings for interference alignment in wireless networks [5, 6]. With A antennas at each node, and constant channels, the achievability of $\lfloor \frac{4A}{3} \rfloor$ DoF was shown by Maddah-Ali, Motahari and Khandani in [5]. Jafar and Shamai showed in [6] that $\frac{4A}{3}$ DoF were achievable when $M > 1$ for constant channels, and also proved that this was the information theoretic outer bound for all M. For the scalar (SISO) case, i.e., $M = 1$, Jafar and Shamai showed that $\frac{4}{3}$ DoF were achievable when the channels were time-varying. The DoF of the SISO case with constant and complex channels were settled in [7] by Cadambe, Jafar and Wang, who introduced asymmetric complex signaling, also known as improper Gaussian signaling and showed that it achieves the optimal value of $\frac{4}{3}$ for the complex SISO X channel. The SISO case with constant and real coefficients was shown to achieve the optimal value of $\frac{4}{3}$ DoF in [8] by Motahari, Gharan and Khandani, who introduced a real interference alignment framework based on rational-independence and diophantine approximation theory. Generalized degrees of freedom (GDoF) results for a symmetric SISO real constant X channel were obtained in [9] by Huang, Jafar and Cadambe, who also found a sufficient condition under which treating interference as noise is capacity optimal in the fully asymmetric case. A capacity approximation for the real SISO constant X channel within a constant gap, subject to a small outage set, was obtained by Niesen and Maddah-Ali in [10] using a novel deterministic channel model. For X networks, i.e., with arbitrary number (M) of transmitters and arbitrary number (N) of receivers, Cadambe and Jafar show in [11] that the SISO setting with time-varying channel coefficients has $\frac{MN}{M+N-1}$ DoF. The result is extended to the real constant SISO setting using the rational independence framework by Motahari et al. in [8]. Partial characterizations of the DoF region are found by Wang in [12]. Cadambe and Jafar show in [13] that the DoF value remains unchanged when relays and feedback

are included. DoF of the time-varying MIMO X channel with $A > 1$ antennas at each node are settled in [14] by Sun et al. who identify a one-sided decomposability property of X networks, and show that the spatial scale invariance conjecture of Wang, Gou and Jafar [15] (that the DoF scale with the number of antennas) holds in this case. The DoF of a layered multihop SISO X channel with 2 source nodes and 2 destination nodes are characterized in [16] by Wang, Gou and Jafar, who show that the DoF can only take the values $1, \frac{4}{3}, \frac{3}{2}, \frac{5}{3}, 2$ and identify the networks that correspond to each value. Note that all the DoF results mentioned above are meant in the 'almost surely' sense, i.e., they hold for almost all channel realizations but in every case there are channels for which the DoF remain unknown. The problem is particularly severe for rational alignment and diophantine approximation based schemes for real constant channels, where while the DoF value applicable to almost all channels is known, the DoF of any given channel realization is unknown for almost all channel realizations.

For wired networks, if intermediate nodes are intelligent, i.e., operations at intermediate nodes can be optimized, then the sum-capacity of an all-unicast network, i.e., an X network, has been shown to be achievable by routing [16]. However, due to practical limitations, optimization of intermediate nodes may not be possible. While the overhead and complexity of learning and optimizing individual coding coefficients at all intermediate nodes may be excessive, it is much easier to learn only the end-to-end channel coefficients, e.g., through network tomography, with no knowledge of the internal structure of the network or the individual coding coefficients at the intermediate nodes. This is the setting that we explore in this work.

2.2 Finite Field X Channel Model

Consider the finite field X channel

$$\begin{aligned} \bar{y}_1(t) &= h_{11}\bar{x}_1(t) + h_{12}\bar{x}_2(t) \\ \bar{y}_2(t) &= h_{22}\bar{x}_2(t) + h_{21}\bar{x}_1(t) \end{aligned}$$

where, over the t^{th} channel use, $\bar{x}_i(t)$ is the symbol sent by source i, h_{ji} represents the channel coefficient between source i and destination j and $\bar{y}_j$ represents the received symbol at destination j. All symbols $\bar{x}_i(t), h_{ji}, \bar{y}_j(t)$ and addition and multiplication operations are in a finite field $\mathbb{F}_{p^n}$. The channel coefficients h_{ji} are constant and assumed to be perfectly known at all sources and destinations. There are four independent messages, with W_{ji} denoting the message that originates at source i and is intended for destination j.

A coding scheme over T channel uses, that assigns to each message W_{ji} a rate R_{ji}, measured in units of $\mathbb{F}_{p^n}$ symbols per channel use, corresponds to an encoding function at each source i that maps the messages originating at that source into a sequence of T transmitted symbols, and a decoding function at each destination j that maps the sequence of T received symbols into decoded messages $\hat{W}_{ji}$.

$$\text{Encoder 1:} \quad (W_{11}, W_{21}) \to \bar{x}_1(1)\bar{x}_1(2)\cdots\bar{x}_1(T) \tag{1}$$

$$\text{Encoder 2:} \quad (W_{12}, W_{22}) \to \bar{x}_2(1)\bar{x}_2(2)\cdots\bar{x}_2(T) \tag{2}$$

$$\text{Decoder 1:} \quad \bar{y}_1(1)\bar{y}_1(2)\cdots\bar{y}_1(T) \to (\hat{W}_{11}, \hat{W}_{12}) \tag{3}$$

$$\text{Decoder 2:} \quad \bar{y}_2(1)\bar{y}_2(2)\cdots\bar{y}_2(T) \to (\hat{W}_{21}, \hat{W}_{22}) \tag{4}$$

Each message W_{ji} is uniformly distributed over $\{1, 2, \cdots, \lceil p^{nTR_{ji}} \rceil\}$, $\forall i, j \in \{1, 2\}$. An error occurs if $(\hat{W}_{11}, \hat{W}_{12}, \hat{W}_{21}, \hat{W}_{22}) \neq (W_{11}, W_{12}, W_{21}, W_{22})$. A rate tuple $(R_{11}, R_{12}, R_{21}, R_{22})$ is said to be

achievable if there exist encoders and decoders such that the probability of error can be made arbitrarily small by choosing a sufficiently large T. The closure of all achievable rate pairs is the capacity region and the maximum value of $R_{11}+R_{12}+R_{21}+R_{22}$ across all rate tuples that belong to the capacity region, is the sum-capacity, that we will refer to as simply the capacity, denoted as C, for brevity. Since we are especially interested in linear interference alignment, we will also define C_{linear} as the highest sum-rate possible through vector linear coding schemes (see, e.g., [17]), also known as linear beamforming schemes, over the base field $\mathbb{F}_p$.

2.3 Zero Channels

First, let us deal with trivial cases where some of the channel coefficients are zero.

Theorem 1 *If one or more of the channel coefficients h_{ji} is equal to zero, the capacity is given as follows.*

1. *If $h_{12}=h_{21}=0$ and $h_{11},h_{22}\neq 0$, then $C=C_{linear}=2$.*
2. *If $h_{11}=h_{22}=0$ and $h_{12},h_{21}\neq 0$, then $C=C_{linear}=2$.*
3. *If $h_{11}=h_{12}=h_{21}=h_{22}=0$, then $C=C_{linear}=0$.*
4. *In all other cases where at least one channel coefficient is zero, $C=C_{linear}=1$.*

Proof: Cases 1, 2, 3 are trivial. The resulting channel for Case 4 is a MAC, BC or Z channel. MAC and BC have capacity 1 by min-cut max-flow theorem, and the proof for the Z channel follows from the corresponding DoF result presented in [6] for the wireless setting.

2.4 X Channel Normalization

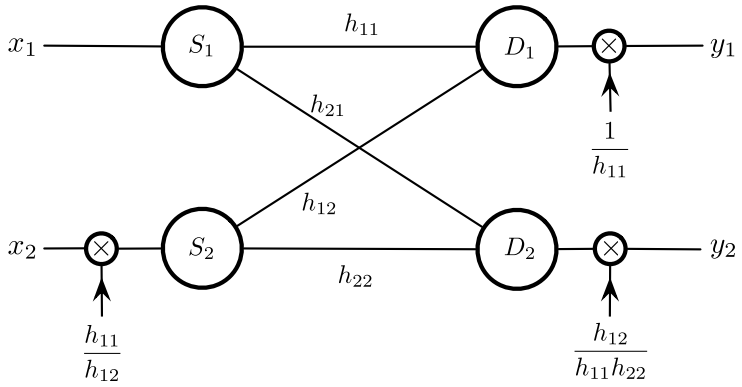

Figure 2: Normalization in X channel

Based on Theorem 1, henceforth we will assume that all channel coefficients are non-zero. We call this the fully connected X channel. Without loss of generality, let us normalize the channel coefficients by invertible operations at the sources and destinations shown in Fig. 2. Since these

are invertible operations, they do not affect the channel capacity:
Destination 1 normalizes symbols by $h_{11} : y_1 = \frac{\bar{y}_1}{h_{11}}$
Destination 2 normalizes symbols by $\frac{h_{11}h_{22}}{h_{12}} : y_2 = \frac{\bar{y}_2 h_{12}}{h_{11}h_{22}}$
Source 2 normalizes symbols by $\frac{h_{11}}{h_{12}}$: $x_2 = \frac{\bar{x}_2 h_{12}}{h_{11}}$
Source 1 performs no normalization : $x_1 = \bar{x}_1$
The normalized X channel is represented as

$$\begin{aligned} y_1 &= x_1 + x_2 \\ y_2 &= hx_1 + x_2 \end{aligned}$$

wherein we have reduced the channel parameters to a single channel coefficient h, defined as

$$h = \frac{h_{12}h_{21}}{h_{11}h_{22}}. \tag{5}$$

All symbols are still over $\mathbb{F}_{p^n}$.

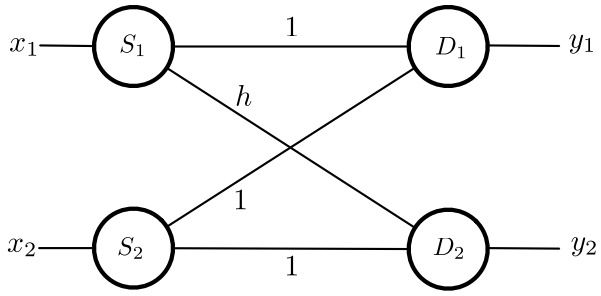

Figure 3: Normalized X channel with Non-Zero Coefficients

2.5 Capacity of the Finite Field X Channel

As mentioned in the review of prior work, the multiple input multiple output (MIMO) wireless X channel where each node is equipped with n antennas has $\frac{4n}{3}$ DoF [6, 7]. For almost all channel realizations in the wireless setting, the DoF are achieved through a linear vector space interference alignment scheme. If n is a multiple of 3, no symbol extensions are needed and spatial beamforming is sufficient. For example, if each node is equipped with 3 antennas, then it suffices to send 1 symbol per message, each along its assigned 3×1 signal vector. The vectors are chosen such that the two undesired symbols at each destination align in the same dimension leaving the remaining 2 dimensions free to resolve the desired signals. If n is not a multiple of 3 then 3 symbol extensions (i.e., coding over 3 channel uses) are needed to create a vector space within which a third of the dimensions are assigned to each message. When translating these insights into the finite field X channel with only scalar inputs and scalar outputs (SISO) we are guided by the main insight presented below.

2.5.1 Insight: MIMO interpretation

The main insight that forms the basis of this work is that *a SISO network over $\mathbb{F}_{p^n}$ is analogous to a $n \times n$ MIMO network, albeit with a special structure imposed on the channel matrix due to finite field arithmetic.*

To appreciate this insight, let us briefly review the fundamentals. The finite field $\mathbb{F}_{p^n}$ can be used to generate an n-dimensional vector space as follows. Each element of $\mathbb{F}_{p^n}$ can be represented in the form

$$z = x_{n-1}s^{n-1} + x_{n-2}s^{n-2} + \ldots + x_1 s^1 + x_0 \tag{6}$$

wherein $z \in \mathbb{F}_{p^n}$, $x_i \in \mathbb{F}_p$.

As an example consider $\mathbb{F}_{3^3}$ which contains 27 elements $\{0, 1, \ldots, 26\}$ and each element $a \in \mathbb{F}_{3^3}$ is of the form $3^2a_2+3a_1+a_0$, wherein $a_2, a_1, a_0 \in \mathbb{F}_3$ with values from {0,1,2}. Hence every element can be written in a vector notation with coefficients $[a_2; a_1; a_0]$, e.g., $a = 22$ can be written as $[2\ ;\ 1\ ;\ 1]$.

Next, let us see how multiplication with the channel coefficient $h \in \mathbb{F}_{3^3}$ is represented as a multiplication with a 3×3 matrix with elements in $\mathbb{F}_3$. Consider the monic irreducible cubic polynomial s^3+2s+1 which is treated as zero in the field. The field itself consists of all polynomials with coefficients in $\mathbb{F}_3$, modulo $s^3 + 2s + 1$. Since $s^3 + 2s + 1 = 0$ in $\mathbb{F}_{3^3}$, it follows that

$$s^3 = -2s - 1 = (3-2)s + (3-1) = s + 2 \tag{7}$$

$$s^4 = s(s^3) = s(s+2) = s^2 + 2s \tag{8}$$

Since $h, x \in \mathbb{F}_{3^3}$ they can be represented as $h = h_2s^2 + h_1s + h_0$, $x = x_2s^2 + x_1s + x_0$ where $h_i, x_i \in \mathbb{F}_{3^3}$. The product $y = hx \in \mathbb{F}_{3^3}$ can be written as

$$\begin{aligned} y = hx &\equiv (h_2s^2 + h_1s + h_0)(x_2s^2 + x_1s + x_0) \\ &= s^4(h_2x_2) + s^3(h_2x_1 + h_1x_2) + s^2(h_2x_0 + h_0x_2 + h_1x_1) + s(h_1x_0 + h_0x_1) + (h_0x_0) \end{aligned} \tag{9}$$

Equivalently,

$$\mathbf{y} = \mathbf{Hx} = \begin{bmatrix} h_2 + h_0 & h_1 & h_2 \\ 2h_2 + h_1 & h_2 + h_0 & h_1 \\ 2h_1 & 2h_2 & h_0 \end{bmatrix} \begin{bmatrix} x_2 \\ x_1 \\ x_0 \end{bmatrix} \tag{10}$$

wherein $\mathbf{x}, \mathbf{y}$ are 3×1 vector with entries from $\mathbb{F}_3$ and $\mathbf{H}$ is a 3×3 matrix with its 9 entries from $\mathbb{F}_3$. Here the equivalence of SISO channel over $\mathbb{F}_{3^3}$ and MIMO channel over $\mathbb{F}_3$ is established through the 3×3 linear transformation, $\mathbf{H}$. Note also the structure inherent in the matrix representation $\mathbf{H}$. While there are 3^9 possible 3×3 matrices over $\mathbb{F}_3$, there are only 27 valid $\mathbf{H}$ matrices, because $\mathbb{F}_{3^3}$ has only 27 elements. This leads us to the main challenge that remains.

2.5.2 Challenge: Channel Structure

Given the main insight, the challenge that remains is dealing with the structural constraints on the MIMO channels that arise due to finite field arithmetic. Structured channels are also encountered in the wireless setting — channels obtained by symbol extensions have a block diagonal structure [6], asymmetric complex signaling based schemes used for the SISO X channel have a unitary matrix structure [7]. Channel structure can be destructive, e.g., loss of capacity in rank deficient channels.

However, channel structure can also be constructive, e.g., diagonal channel matrices enable the CJ scheme in [4], and certain types of rank deficiencies have been shown to facilitate simpler alternatives to interference alignment schemes [18]. On the one hand, the MIMO channels, which arise by viewing $\mathbb{F}_{p^n}$ as an n dimensional vector space over $\mathbb{F}_p$, have a structure that is neither diagonal nor unitary. On the other hand, diagonal channel matrices, unitary channel matrices, as well as the finite field channel matrices, all have the property that matrix multiplication is commutative, which can be a very useful property for interference alignment schemes. The impact of channel structure in the SISO constant finite field X channel setting is therefore an intriguing question.

2.5.3 Main Result

The capacity result for the finite field X channel is presented in the following theorem.

Theorem 2 *For the fully connected X channel over $\mathbb{F}_{p^n}$, with $p > 2$, if*

$$h = \frac{h_{12}h_{21}}{h_{11}h_{22}} \notin \mathbb{F}_p \tag{11}$$

then

$$C \;=\; C_{linear} = \frac{4}{3} \tag{12}$$

in units of $\mathbb{F}_{p^n}$ symbols per channel use. If $h \in \mathbb{F}_p$, then $C_{linear} = 1$.

The setting where $h \in \mathbb{F}_p$ corresponds to the real constant SISO wireless X channel. Linear DoF collapse in this setting because even with symbol extensions, the channel matrices are simply scaled identity matrices so that the alignment of vector spaces is identical at both receivers, making it impossible to have signals align at one receiver where they are undesired and remain resolvable at the other receiver where they are desired. Since $h \in \mathbb{F}_p$ is the only exception where the capacity falls short of 4/3, it is evident from Theorem 2 that the capacity results for the 2 user finite field constant X over $\mathbb{F}_{p^n}$ closely mirror the corresponding DoF results for the real MIMO X channel where each user has n antennas. Remarkably, even though the channels in the finite field setting are highly structured, the structural constraints do not impact the capacity result. The significance of channel structure will become transparent when we study the 3 user interference channel later in this paper.

Note that there are $p^n - 1$ possible non-zero values for h, out of which all but $p - 1$ have the capacity value of $\frac{4}{3}$ which is achieved by linear beamforming. The fraction of degenerate fully connected channel instances, for which $C_{\text{linear}} = 1$, is therefore as follows.

$$\frac{(p-1)}{(p^n-1)} = \frac{1}{1 + p + p^2 + \cdots + p^{n-1}} \tag{13}$$

which approaches 0 as $p \to \infty$. Note the similarity with the constant X channel in the wireless setting for which Cadambe et al. have shown in [7] for the complex case and Motahari et al. have shown in [8] for the real case, that interference alignment scheme achieves 4/3 DoF for *almost all* channel realizations. Remarkably, in the finite field case the fraction of channels with linear capacity $\frac{4}{3}$ is non-trivial and still precisely computable. While a tangible connection seems elusive,

it is an intriguing thought, whether interpreting p and n in (13) as analogous to finite SNR and finite diversity in the wireless setting might lead to finer insights there that are not available directly from the coarse DoF metric.

Proof: The information theoretic outer bound of $\frac{4}{3}$ follows immediately from the DoF outer bound for the wireless setting presented in [6], a combination of the Z channel bounds, with minor adjustments to account for finite field channels. The linear capacity bound of 1 when $h \in \mathbb{F}_p$ is also straightforward because in this case, regardless of the number of channel extensions, all channel matrices are simply scaled identity matrices. Since the scaling factors are irrelevant for vector spaces, i.e., beamforming schemes, the linear capacity is not changed if we replace all channel gains with unity. But such a channel has only rank 1 (equivalently min-cut value of 1) per channel use, so its sum-rate is bounded by 1, which is therefore also an outer bound for linear capacity on the original channel. Achievability of rate 1 is trivial in a fully connected X channel. So this leaves us only to prove that a sum rate of $\frac{4}{3}$ is achievable through vector linear schemes when $h \notin \mathbb{F}_p$. The achievability scheme is the simplest, i.e., no symbol extensions are required and only scalar linear coding (one stream per message) is sufficient, when n is 3. For ease of exposition, the achievability proof for this case, i.e., for the X channel over $\mathbb{F}_{p^3}$ is presented first, in Section 2.6 (an alternate proof for $\mathbb{F}_{p^3}$ is also presented in Appendix I). The achievability proof over $\mathbb{F}_{p^2}$, which requires a slightly different approach, is presented in Appendix II. The proofs over $\mathbb{F}_{p^3}$ and $\mathbb{F}_{p^2}$ are *not restricted* to $p > 2$. The achievability proof for the remaining general case, over $\mathbb{F}_{p^n}$, $p > 2$, is presented in Section 2.7. ■

2.6 Achievability over $\mathbb{F}_{p^3}$

Proof: Consider the normalized X channel which can be characterized by single channel coefficient $h = \frac{h_{12}h_{21}}{h_{11}h_{22}}$ from $\mathbb{F}_{p^3}$. We use superposition coding at the sources, wherein messages from source 1, (W_{11}, W_{21}) are independently encoded into symbols x_{11}, x_{21}, respectively, and added to obtain the transmitted symbol $x_1 = x_{11} + x_{21}$ and messages from source 2, (W_{12}, W_{22}) are similarly encoded as $x_2 = x_{21} + x_{22}$. Symbols x_{ji} are from the subfield $\mathbb{F}_p$. The received symbols are expressed as

$$\begin{aligned} y_1 &= x_{11} + x_{12} + x_{22} + x_{21} \\ y_2 &= hx_{21} + hx_{11} + x_{22} + x_{12} \end{aligned}$$

wherein $h, y_j \in \mathbb{F}_{p^3}$.

As described earlier, $\mathbb{F}_{p^3}$ can be split into a 3-dimensional space over subfield $\mathbb{F}_p$ so that the output has 3 dimensions (each over $\mathbb{F}_p$) within which 2 desired symbols and 2 interference symbols are present at each destination. To achieve capacity, the 2 interference symbols should be aligned at each destination such that they occupy only one dimension at that destination while remaining distinguishable at the other destination where they are desired. To this end, we will assign a precoding "vector" $v_{ji} \in \mathbb{F}_{p^3}$ to each symbol x_{ji}.

$$\begin{aligned} y_1 &= v_{11}x_{11} + v_{12}x_{12} + v_{22}x_{22} + v_{21}x_{21} \\ y_2 &= v_{22}x_{22} + hv_{21}x_{21} + hv_{11}x_{11} + v_{12}x_{12} \end{aligned}$$

Equivalently, using vector notation,

$$\begin{aligned} \mathbf{y}_1 &= \mathbf{v}_{11}x_{11} + \mathbf{v}_{12}x_{12} + \mathbf{v}_{22}x_{22} + \mathbf{v}_{21}x_{21} \\ \mathbf{y}_2 &= \mathbf{v}_{22}x_{22} + \mathbf{H}\mathbf{v}_{21}x_{21} + \mathbf{H}\mathbf{v}_{11}x_{11} + \mathbf{v}_{12}x_{12} \end{aligned}$$

wherein $\mathbf{y}_j, \mathbf{v}_{ji} \in \mathbb{F}_p^{3\times 1}$ are 3×1 vectors with entries from $\mathbb{F}_p$ and $\mathbf{H} \in \mathbb{F}_p^{3\times 3}$ is a structured 3×3 matrix with elements from $\mathbb{F}_p$, representing $h \in \mathbb{F}_{p^3}$.
Interference alignment conditions are expressed as

$$\begin{aligned} \text{span}(\mathbf{v}_{22}) &= \text{span}(\mathbf{v}_{21}) && (14)\\ \text{span}(\mathbf{v}_{12}) &= \text{span}(\mathbf{H}\mathbf{v}_{11}) && (15)\end{aligned}$$

This is accomplished by setting

$$\begin{aligned} \mathbf{v}_{22} &= \mathbf{v}_{21} && (16)\\ \mathbf{v}_{12} &= \mathbf{H}\mathbf{v}_{11} && (17)\end{aligned}$$

so that interference is aligned at each destination along one dimension. For ease of exposition, an instance of the problem and its solution are illustrated in Fig. 4 using scalar notation and again in Fig. 5 using vector notation.

At the destinations, the spaces occupied by the two desired symbols and the aligned interference symbol are represented using matrices S_1 (for destination 1) and S_2 (for destination 2).

$$S_1 = [v_{11} \quad v_{12} \quad v_{21}] = [v_{11} \quad hv_{11} \quad v_{21}] \tag{18}$$
$$S_2 = [v_{22} \quad hv_{21} \quad v_{12}] = [v_{21} \quad hv_{21} \quad hv_{11}] \tag{19}$$

When $h \notin \mathbb{F}_p$, we will now show that we can choose v_{11} and v_{21} such that elements of S_1 and S_2 are linearly independent over $\mathbb{F}_p$. Set $v_{21} = 1$. Then S_1 and S_2 can be written as

$$S_1 = [v_{11} \quad hv_{11} \quad 1] \qquad \& \qquad S_2 = [1 \quad h \quad hv_{11}] \tag{20}$$

Consider S_1. Note that $\mathbf{v}_{11}$ and $\mathbf{H}\mathbf{v}_{11}$, or equivalently v_{11} and hv_{11}, are linearly independent over $\mathbb{F}_p$ since $h \notin \mathbb{F}_p$, i.e., $\mathbf{H}$ is not a scaled identity matrix. Hence elements of S_1 are linearly independent if 1 is not a linear combination of v_{11} and hv_{11}, or equivalently, if $\frac{1}{v_{11}}$ is not a linear combination (with coefficients from $\mathbb{F}_p$) of 1 and h. This is guaranteed if

$$v_{11} \notin A \triangleq \left\{ \frac{1}{\alpha + \beta h} : \alpha, \beta \in \mathbb{F}_p, (\alpha, \beta) \neq (0,0) \right\} \cup \{0\} \tag{21}$$

Similarly, consider S_2. Note that 1 and h are linearly independent over $\mathbb{F}_p$, since $\mathbf{H}$ is not a scaled identity matrix. Hence, elements of S_2 are linearly independent if hv_{11} is not a linear combination of 1 and h over $\mathbb{F}_p$, or equivalently, if v_{11} is not a linear combination of $\frac{1}{h}$ and 1 over $\mathbb{F}_p$. This is guaranteed if

$$v_{11} \notin B \triangleq \left\{ \alpha + \frac{\beta}{h} : \alpha, \beta \in \mathbb{F}_p, (\alpha, \beta) \neq (0,0) \right\} \cup \{0\} \tag{22}$$

Since $|A| \leq p^2$ and $|B| \leq p^2$, and all p constant polynomials are contained in both A and B, we must have

$$|A \cup B| \leq 2p^2 - p \tag{23}$$

Unless $A \cup B$ contains all p^3 elements of $\mathbb{F}_{p^3}$ there is at least one choice of v_{11} that satisfies both (21) and (22). In other words, the scheme works if

$$p^3 > 2p^2 - p \tag{24}$$

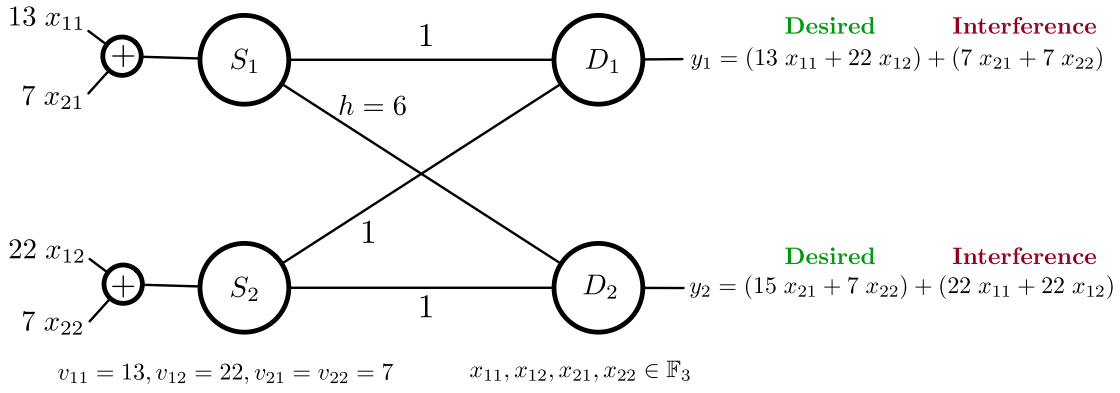

Figure 4: An instance of the X channel over $\mathbb{F}_{3^3}$ and its capacity optimal solution represented in scalar notation.

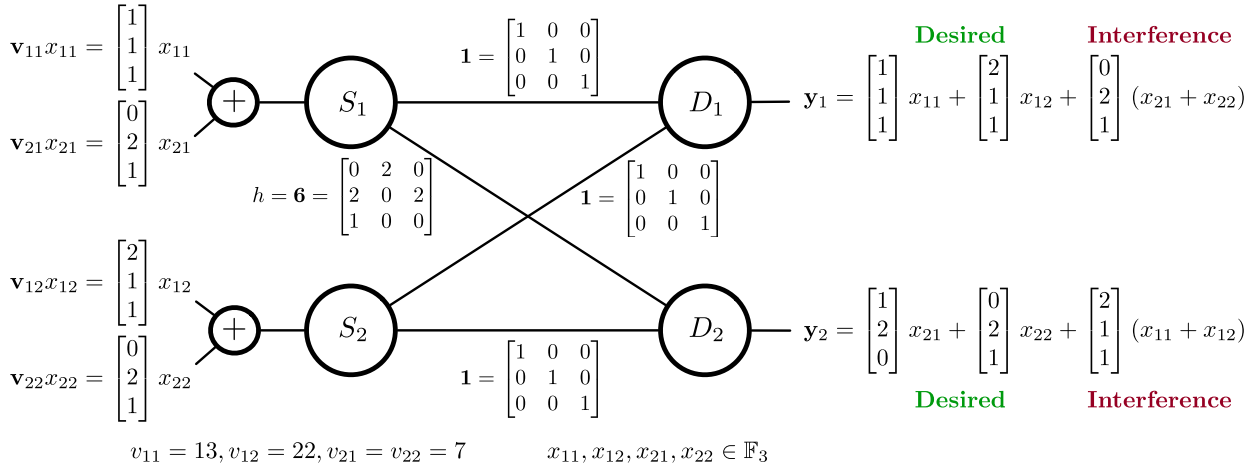

Figure 5: The same example and solution as Fig. 4, illustrated in vector notation.

which is true for all $p \geq 2$. Thus, we have proved the achievability of rate $\frac{1}{3}$ per message, and a sum-rate of $\frac{4}{3}$, which matches the capacity outer bound. Note that a $\mathbb{F}_{p^3}$ symbol represents $\frac{1}{3}$ of an $\mathbb{F}_p$ symbol and the capacity is measured in $\mathbb{F}_{p^3}$ units because the original channel alphabet is from $\mathbb{F}_{p^3}$. Also note that the achievability proof applies to $p = 2$ as well. An alternate proof for achievability of sum-rate of $\frac{4}{3}$ is presented in Appendix I. ■

Similar to splitting a field $\mathbb{F}_{p^3}$ to form a 3-dimensional space in field of order p, other fields of order p^n can be split to a n-dimensional field of order p. However, in order to achieve the optimal capacity of $\frac{4}{3}$, symbol extensions would be required when n is not a multiple of 3. The capacity result for the general case is presented in the next section.

2.7 Achievability over $\mathbb{F}_{p^n}$

Proof: Achievability proof for channels over field $\mathbb{F}_{p^2}$ is presented in Appendix II. Here, we discuss achievability proof for channels over field $\mathbb{F}_{p^n}, n > 3$.
Let us use 3 symbol extensions, so that we operate in a $3n$ dimensional vector space over $\mathbb{F}_p$. Each message W_{ji} is encoded into n streams represented by the elements of the column vector $x_{ji} \in \mathbb{F}_p^{n\times 1}$, and the n streams are sent along the n column vectors of the precoding matrix $\mathbf{v}_{ji} \in \mathbb{F}_p^{3n\times n}$, or equivalently, $v_{ji} \in \mathbb{F}_{p^n}^{3\times n}$. Thus, the sum data rate is $\frac{4}{3}$ in units of $\mathbb{F}_{p^n}$ symbols per channel use, and it remains to be shown that the desired symbols are resolvable from interference at each destination. Over each extended channel use, the received signals, $y_1, y_2 \in \mathbb{F}_{p^n}^{3\times 1}$ at each destination are expressed as:

$$\begin{aligned} y_1 &= v_{11}x_{11} + v_{12}x_{12} + v_{22}x_{22} + v_{21}x_{21} \\ y_2 &= v_{22}x_{22} + hv_{21}x_{21} + hv_{11}x_{11} + v_{12}x_{12} \end{aligned}$$

Equivalently, using vector notation the received signals, $\mathbf{y}_1, \mathbf{y}_2 \in \mathbb{F}_p^{3n\times 1}$ at each destination are expressed as:

$$\begin{aligned} \mathbf{y}_1 &= \mathbf{v}_{11}x_{11} + \mathbf{v}_{12}x_{12} + \mathbf{v}_{22}x_{22} + \mathbf{v}_{21}x_{21} \\ \mathbf{y}_2 &= \mathbf{v}_{22}x_{22} + \mathbf{H}\mathbf{v}_{21}x_{21} + \mathbf{H}\mathbf{v}_{11}x_{11} + \mathbf{v}_{12}x_{12} \end{aligned}$$

wherein $\mathbf{H} \in \mathbb{F}_p^{3n\times 3n}$ is the channel matrix. Interference alignment conditions are expressed as

$$\text{span}(\mathbf{v}_{22}) = \text{span}(\mathbf{v}_{21}) \quad (25)$$
$$\text{span}(\mathbf{v}_{12}) = \text{span}(\mathbf{H}\mathbf{v}_{11}) \quad (26)$$

This is accomplished by setting

$$\mathbf{v}_{22} = \mathbf{v}_{21} \quad (27)$$
$$\mathbf{v}_{12} = \mathbf{H}\mathbf{v}_{11} \quad (28)$$

At each destination, $2n$ desired symbols and n aligned interference symbols are represented using matrices $S_1 \in \mathbb{F}_{p^n}^{3\times 3n}$ (for destination 1) and $S_2 \in \mathbb{F}_{p^n}^{3\times 3n}$ (for destination 2).

$$S_1 = [v_{11} \quad v_{12} \quad v_{21}] = [v_{11} \quad hv_{11} \quad v_{21}] \quad (29)$$
$$S_2 = [v_{22} \quad hv_{21} \quad v_{12}] = [v_{21} \quad hv_{21} \quad hv_{11}] \quad (30)$$

We will now show that when $h \notin \mathbb{F}_p$, we can choose v_{11} and v_{21} such that the columns of S_1 and S_2 are linearly independent over $\mathbb{F}_p$. Let us choose

$$v_{11} = gv_{21} \quad (31)$$

with a non-zero $g \in \mathbb{F}_{p^n}$. For notational convenience, we will denote v_{21} as just $v \in \mathbb{F}_{p^n}^{3\times n}$. Then S_1 and S_2 can be written as

$$S_1 = [gv \quad hgv \quad v] \quad (32)$$
$$S_2 = [v \quad hv \quad hgv] \quad (33)$$

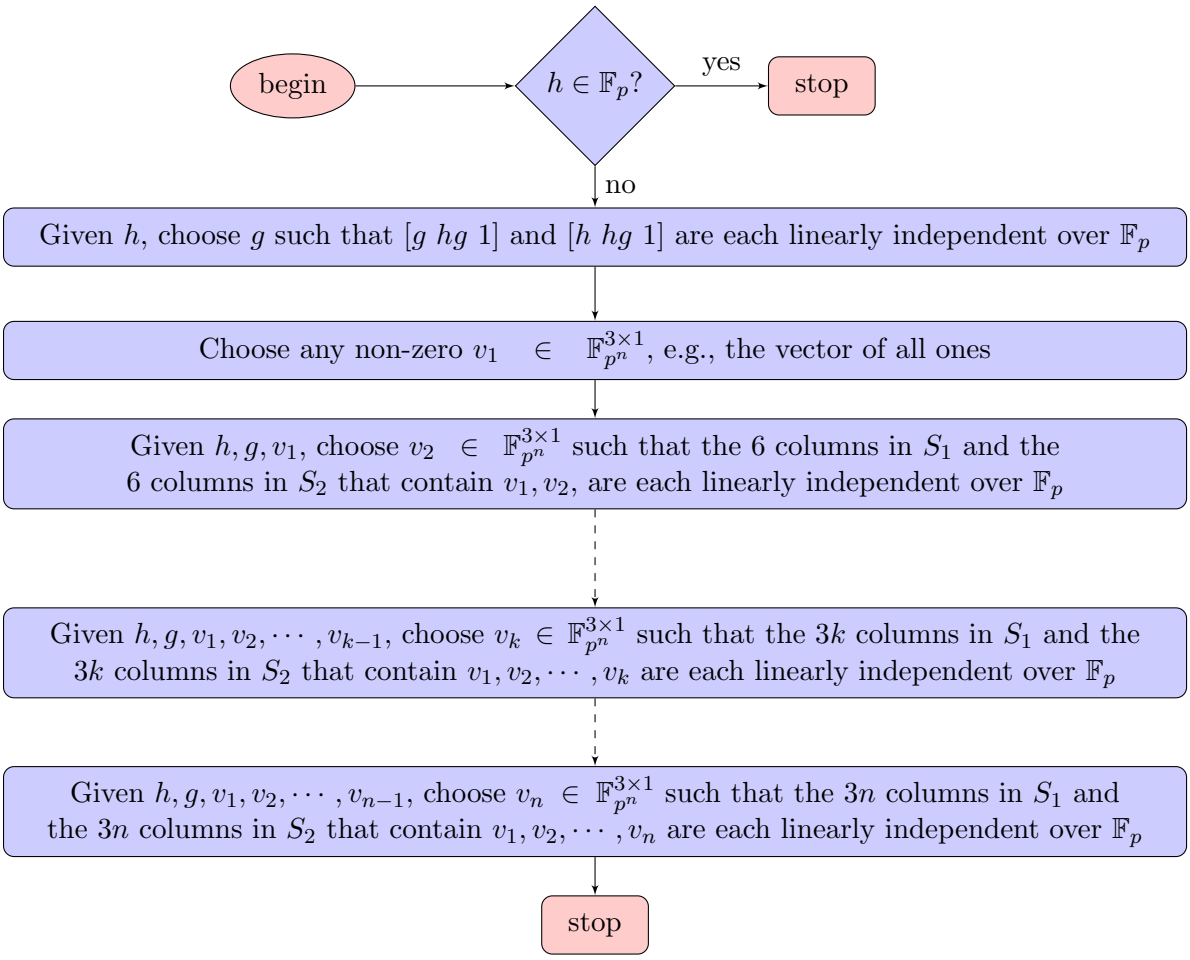

Figure 6: Algorithm for the construction of precoding vectors.

wherein beamforming matrix v has n columns, denoted as $v_1, \ldots, v_n \in \mathbb{F}_{p^n}^{3\times 1}$.

$$S_1 = [gv_1 \ldots gv_n \quad hgv_1 \ldots hgv_n \quad v_1 \ldots v_n] \tag{34}$$
$$S_2 = [hv_1 \ldots hv_n \quad hgv_1 \ldots hgv_n \quad v_1 \ldots v_n] \tag{35}$$

In Fig. 6, we illustrate the recursive proof described hereafter.

Choose v_1 as the all-ones vector. We first consider columns containing v_1. There are three such columns, and they need to be linearly independent in both S_1 and S_2. This requires that following vectors are linearly independent over $\mathbb{F}_p$.

$$\text{From } S_1 : [gv_1 \quad hgv_1 \quad v_1] \tag{36}$$
$$\text{From } S_2 : [v_1 \quad hv_1 \quad hgv_1] \tag{37}$$

Consider S_1. Note that gv_1 and hgv_1 are linearly independent over $\mathbb{F}_p$, since $h \notin \mathbb{F}_p$, i.e., h is not a constant polynomial, and $g, v_1 \neq 0$. Hence, elements of S_1 are linearly independent over $\mathbb{F}_p$ if 1 is not a linear combination of g and hg over $\mathbb{F}_p$, or equivalently, $\frac{1}{g}$ is not a linear combination

of 1 and h over $\mathbb{F}_p$. This is guaranteed if

$$g \notin A \triangleq \left\{ \frac{1}{\alpha + \beta h} : \alpha, \beta \in \mathbb{F}_p, (\alpha, \beta) \neq (0,0) \right\} \cup \{0\} \tag{38}$$

Similarly, consider S_2. Note that v_1 and hv_1 are linearly independent, since $h \notin \mathbb{F}_p$, i.e., h is not a constant polynomial. Hence elements of S_2 are linearly independent over $\mathbb{F}_p$ if hg is not a linear combination of 1 and h over $\mathbb{F}_p$, or equivalently, g is not a linear combination of 1 and $\frac{1}{h}$ over $\mathbb{F}_p$. This is guaranteed if

$$g \notin B \triangleq \left\{ \alpha + \frac{\beta}{h} : \alpha, \beta \in \mathbb{F}_p, (\alpha, \beta) \neq (0,0) \right\} \cup \{0\} \tag{39}$$

Since $|A| \leq p^2, |B| \leq p^2$ and A and B both contain all p elements of $\mathbb{F}_p$, we must have $|A \cup B| \leq 2p^2 - p$. Therefore, a choice of g that satisfies both (38) and (39) is guaranteed to exist if

$$p^n > 2p^2 - p \tag{40}$$

which is true $\forall n \geq 3$.

If $v_k \neq 0$, the same choice of g ensures that the following columns from S_1 and S_2 are linearly independent over $\mathbb{F}_p$, $\forall k \in \{1, \ldots, n\}$.

$$\text{From } S_1 : [gv_k \quad hgv_k \quad v_k] \tag{41}$$
$$\text{From } S_2 : [v_k \quad hv_k \quad hgv_k] \tag{42}$$

We now present the recursive proof for linear independence over $\mathbb{F}_p$ of desired and interference symbols at destinations. At iteration k, column vector v_{k+1} will be chosen based on previously chosen columns $v_1, \ldots, v_k$ and g. We already chose v_1 to be the vector of ones. So now v_2 will be chosen such that following columns are linearly independent over $\mathbb{F}_p$ in S_1 and S_2 :

$$\text{From } S_1 : [gv_1 \quad hgv_1 \quad v_1 \quad gv_2 \quad hgv_2 \quad v_2] \tag{43}$$
$$\text{From } S_2 : [hv_1 \quad hgv_1 \quad v_1 \quad hv_2 \quad hgv_2 \quad v_2] \tag{44}$$

Linear independence over $\mathbb{F}_p$ for (43) and (44) is guaranteed, respectively, if

$$v_2 \notin A \triangleq \left\{ \left(\frac{\alpha_1 g + \alpha_2 hg + \alpha_3}{\alpha_4 g + \alpha_5 hg + \alpha_6} \right) v_1 : \alpha_1, \cdots, \alpha_6 \in \mathbb{F}_p, (\alpha_4, \alpha_5, \alpha_6) \neq (0,0,0) \right\} \tag{45}$$
$$v_2 \notin B \triangleq \left\{ \left(\frac{\beta_1 h + \beta_2 hg + \beta_3}{\beta_4 h + \beta_5 hg + \beta_6} \right) v_1 : \beta_1, \cdots, \beta_6 \in \mathbb{F}_p, (\beta_4, \beta_5, \beta_6) \neq (0,0,0) \right\} \tag{46}$$

Now we note that

$$A \cap B \supseteq \left\{ \left(\frac{\beta_2 hg + \beta_3}{\beta_5 hg + \beta_6} \right) v_1 : \beta_1, \cdots, \beta_6 \in \mathbb{F}_p, (\beta_5, \beta_6) \neq (0,0) \right\} \tag{47}$$
$$|A| \leq \frac{(p^3-1)p^3}{p-1} = p^5 + p^4 + p^3 \tag{48}$$
$$|B| - |A \cap B| \leq \frac{(p^3-1)p^3}{p-1} - \frac{(p^2-1)p^2}{p-1} = p^5 + p^4 - p^2 \tag{49}$$
$$|A \cup B| = |A| + |B| - |A \cap B| \leq 2p^5 + 2p^4 + p^3 - p^2 \tag{50}$$

Since there are p^{3n} possible choices for v_2, there must exist at least one choice that satisfies both (45) and (46) if

$$p^{3n} \quad > \quad 2p^5 + 2p^4 + p^3 - p^2 \tag{51}$$

which is true for all $p \geq 3$.

Similarly this recursion is carried out for choosing vectors $v_3, \ldots, v_{n-1}$. We will now describe the last stage of recursion, i.e., choosing vector v_n for given $h, g, v_1, \ldots, v_{n-1}$. We want to design v_n such that all $3n$ columns are linearly independent over $\mathbb{F}_p$ in S_1 and S_2 :

$$\text{From } S_1 : [gv_1 \quad hgv_1 \quad v_1 \quad gv_2 \quad hgv_2 \quad v_2 \quad \ldots \quad gv_n \quad hgv_n \quad v_n] \tag{52}$$

$$\text{From } S_2 : [hv_1 \quad hgv_1 \quad v_1 \quad hv_2 \quad hgv_2 \quad v_2 \quad \ldots \quad hv_n \quad hgv_n \quad v_n] \tag{53}$$

The linear independence over $\mathbb{F}_p$ is guaranteed if

$$v_n \notin A \quad \triangleq \quad \left\{ \sum_{l=1}^{n-1} \left(\frac{\alpha_{3l-2}g + \alpha_{3l-1}hg + \alpha_{3l}}{\alpha_{3n-2}g + \alpha_{3n-1}hg + \alpha_{3n}} \right) v_l : \alpha_1, \cdots, \alpha_{3n} \in \mathbb{F}_p, (\alpha_{3n-2}, \alpha_{3n-1}, \alpha_{3n}) \neq (0,0,0) \right\} \tag{54}$$

$$v_n \notin B \quad \triangleq \quad \left\{ \sum_{l=1}^{n-1} \left(\frac{\beta_{3l-2}h + \beta_{3l-1}hg + \beta_{3l}}{\beta_{3n-2}h + \beta_{3n-1}hg + \beta_{3n}} \right) v_l : \beta_1, \cdots, \beta_{3n} \in \mathbb{F}_p, (\beta_{3n-2}, \beta_{3n-1}, \beta_{3n}) \neq (0,0,0) \right\} \tag{55}$$

$$\Rightarrow A \cap B \quad \supseteq \quad \left\{ \sum_{l=1}^{n-1} \left(\frac{\beta_{3l-1}hg + \beta_{3l}}{\beta_{3n-1}hg + \beta_{3n}} \right) v_l : \beta_1, \cdots, \beta_{3n} \in \mathbb{F}_p, (\beta_{3n-1}, \beta_{3n}) \neq (0,0) \right\} \tag{56}$$

Next we bound the cardinalities as follows.

$$|A| \quad \leq \quad \frac{(p^3-1)p^{3n-3}}{p-1} = p^{3n-1} + p^{3n-2} + p^{3n-3} \tag{57}$$

$$\begin{aligned} |B| - |A \cap B| \quad &\leq \quad \frac{(p^3-1)p^{3n-3}}{p-1} - \frac{(p^2-1)p^{2n-2}}{p-1} \\ &= \quad p^{3n-1} + p^{3n-2} + p^{3n-3} - p^{2n-1} - p^{2n-2} \end{aligned} \tag{58}$$

$$|A \cup B| = |A| + |B| - |A \cap B| \quad \leq \quad 2p^{3n-1} + 2p^{3n-2} + 2p^{3n-3} - p^{2n-1} - p^{2n-2} \tag{59}$$

Since there are p^{3n} possible choices for v_n, there must exist at least one choice that satisfies both (54) and (55) if

$$p^{3n} \quad > \quad 2p^{3n-1}(1 + \frac{1}{p} + \frac{1}{p^2}) - p^{2n-1} - p^{2n-2} \tag{60}$$

which is easily shown to be true for all $p \geq 3$ as follows. If $p \geq 3$ then the RHS is bounded above by $2p^{3n-1}(1 + \frac{1}{3} + \frac{1}{9}) = \frac{26}{9}p^{3n-1}$ whereas the LHS is bounded below by $3p^{3n-1}$. ■

3 Interference Channel

As noted previously, the impact of channel structure due to finite field operations in $\mathbb{F}_{p^n}$ is not evident in the capacity of the X channel as characterized in Theorem 2, because the capacity results for the $\mathbb{F}_{p^n}$ channels mimic the DoF results for the generic $\mathbb{R}^{n\times n}$ real MIMO X channels in the wireless setting. In this section we will extend our study beyond the X channel, to the 3 user interference channel, where the distinction between a generic $\mathbb{R}^{n\times n}$ MIMO setting and the $\mathbb{F}_p^{n\times n}$ MIMO representations of the finite field $\mathbb{F}_{p^n}$ becomes evident. In particular, we will study the linear sum-capacity, C_{linear}, of a finite field 3-user interference channel with 3 source nodes, 3 destination nodes and 3 independent messages as illustrated in Fig. 7.

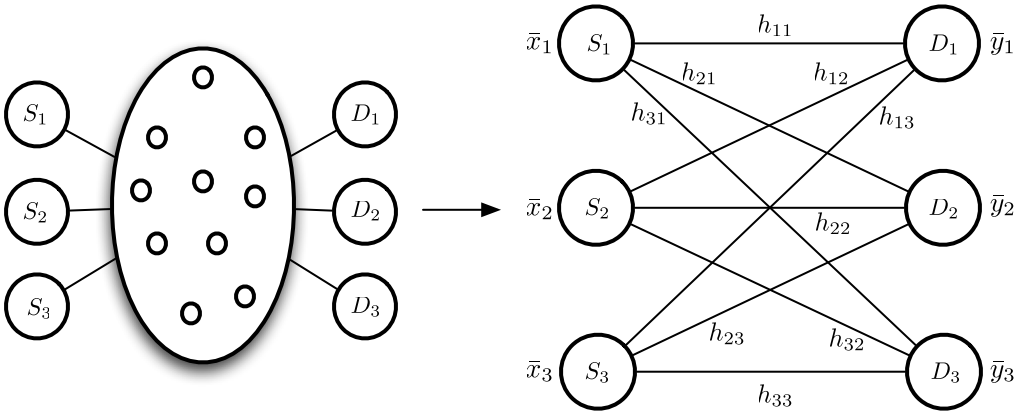

Figure 7: Wired network modeled as 3-user interference channel

3.1 Prior Work

The K user interference channel, with $K > 2$, has been extensively studied in recent years. Cadambe and Jafar showed in [4] that the K-user fully connected interference channel with M antennas at each node has $\frac{MK}{2}$ sum-DoF over a time-varying or frequency-selective channel, based on the CJ scheme. The DoF value of the 3 user constant complex MIMO interference channel with $M > 1$ antennas at each node was also shown by Cadambe and Jafar, to be $\frac{3M}{2}$ using an eigenvector solution. The DoF of asymmetric MIMO settings were characterized in [15, 19–21] and the linear capacity of generic MIMO interference channels without symbol extensions was studied in [15, 22–28].

For the complex constant 3 user SISO interference channel, Cadambe et al. showed in [7] that the linear DoF value is $\frac{6}{5}$ using asymmetric complex signaling scheme which precodes the real and imaginary parts of the signal separately. The constant complex SISO channel setting can be interpreted as having diversity 2. Bresler and Tse characterized the DoF of the 3-user time-varying/frequency-selective interference channel as a function of the channel diversity, L, in [29]. While DoF of $\frac{3}{2}$ can be achieved over channel with infinite diversity, Bresler and Tse showed that the linear DoF of the 3-user interference channel with channel diversity L, is $\frac{3D}{2D+1}$ where

$D = 2L - \lfloor L/2 \rfloor - 1$ is known as the alignment depth. Channel diversity, L, was shown to limit the extent to which interference signals can be aligned while maintaining the resolvability of the desired signals from interference.

In the context of network coding, the 3 unicast problem which is the counterpart of the 3 user interference channel, was studied in [1–3] by Das et al., Ramakrishnan et al., and Meng et al., who introduced the Precoding-Based Network Alignment (PBNA) framework and found conditions under which half the source-destination min-cut was achievable for each user. The results were extended to networks with delay in [30]. These works require time-varying channel coefficients due to a direct translation from the CJ scheme originally designed for the time-varying interference channel. However, in this work we will focus only on the constant channel setting over $\mathbb{F}_{p^n}$, viewed as a constant $\mathbb{F}_p^{n\times n}$ MIMO setting. In particular, we wish to understand the significance of the channel structure.

3.2 Finite Field Interference Channel Model

Consider the finite field 3-user interference channel

$$\begin{aligned}
\bar{y}_1(t) &= h_{11}\bar{x}_1(t) + h_{12}\bar{x}_2(t) + h_{13}\bar{x}_3(t) \\
\bar{y}_2(t) &= h_{21}\bar{x}_1(t) + h_{22}\bar{x}_2(t) + h_{23}\bar{x}_3(t) \\
\bar{y}_3(t) &= h_{31}\bar{x}_1(t) + h_{32}\bar{x}_2(t) + h_{33}\bar{x}_3(t)
\end{aligned}$$

where, over the t^{th} channel use, $\bar{x}_i(t)$ is the symbol sent by source i, h_{ji} represents channel coefficient between source i and destination j and $\bar{y}_j$ represents the received symbol at destination j. All symbols $\bar{x}_i(t), h_{ji}, \bar{y}_j(t)$ and addition and multiplication operations are in a finite field $\mathbb{F}_{p^n}$. The channel coefficients h_{ji} are constant across t channel uses and assumed to be perfectly known at all sources and destinations. There are three independent messages, with W_i denoting the message that originates at source i and is intended for destination i.

A coding scheme over T channel uses, that assigns to each message W_i a rate R_i, measured in units of $\mathbb{F}_{p^n}$ symbols per channel use, corresponds to a encoding function at each source i that maps the messages originating at that source into a sequence of T transmitted symbols, and a decoding function at each destination that maps the sequence of T received symbols into decoded messages $\hat{W}_i$.

$$\text{Encoder 1:} \quad (W_1) \to \bar{x}_1(1)\bar{x}_1(2)\cdots\bar{x}_1(T) \tag{61}$$
$$\text{Encoder 2:} \quad (W_2) \to \bar{x}_2(1)\bar{x}_2(2)\cdots\bar{x}_2(T) \tag{62}$$
$$\text{Encoder 3:} \quad (W_3) \to \bar{x}_3(1)\bar{x}_3(2)\cdots\bar{x}_3(T) \tag{63}$$
$$\text{Decoder 1:} \quad \bar{y}_1(1)\bar{y}_1(2)\cdots\bar{y}_1(T) \to (\hat{W}_1) \tag{64}$$
$$\text{Decoder 2:} \quad \bar{y}_2(1)\bar{y}_2(2)\cdots\bar{y}_2(T) \to (\hat{W}_2) \tag{65}$$
$$\text{Decoder 3:} \quad \bar{y}_3(1)\bar{y}_3(2)\cdots\bar{y}_3(T) \to (\hat{W}_3) \tag{66}$$

Each message W_i is uniformly distributed over $\{1, 2, \cdots, \lceil p^{nTR_i} \rceil\}$, $\forall i \in \{1, 2, 3\}$. An error occurs if $(\hat{W}_1, \hat{W}_2, \hat{W}_3) \neq (W_1, W_2, W_3)$. A rate tuple (R_1, R_2, R_3) is said to be achievable if there exist encoders and decoders such that the probability of error can be made arbitrarily small by choosing a sufficiently large T. The closure of all achievable rate pairs is the capacity region and the maximum value of $R_1 + R_2 + R_3$ across all rate tuples that belong to the capacity region, is the sum-capacity, C. Since we are interested in linear interference alignment, we will again define *linear* capacity,

C_{linear}, as the highest sum-rate possible through vector linear coding schemes over the base field $\mathbb{F}_p$.

3.3 Interference Channel Normalization

As noted in the X channel, since the main insights come from the fully connected setting, we will assume that all channel coefficients are non-zero. Channel settings where some of the channels are zero are dealt with separately in the Appendix III. Without loss of generality, let us normalize the channel coefficients by invertible operations at the sources and destinations shown in Fig. 8. Since these are invertible operations, they do not affect the channel capacity:

Destination 1 normalizes symbols by h_{12} : $y_1 = \frac{\bar{y}_1}{h_{12}}$

Destination 2 normalizes symbols by $\frac{h_{12}h_{23}}{h_{13}}$: $y_2 = \frac{\bar{y}_2 h_{13}}{h_{12}h_{23}}$

Destination 3 normalizes symbols by $\frac{h_{12}h_{23}h_{31}}{h_{21}h_{13}}$: $y_3 = \frac{\bar{y}_3 h_{21}h_{13}}{h_{12}h_{23}h_{31}}$

Source 1 normalizes symbols by $\frac{h_{13}h_{21}}{h_{12}h_{23}}$: $x_1 = \frac{\bar{x}_1 h_{12}h_{23}}{h_{13}h_{21}}$

Source 2 performs no normalization : $x_2 = \bar{x}_2$

Source 3 normalizes symbols by $\frac{h_{13}}{h_{12}}$: $x_3 = \frac{\bar{x}_3 h_{12}}{h_{13}}$

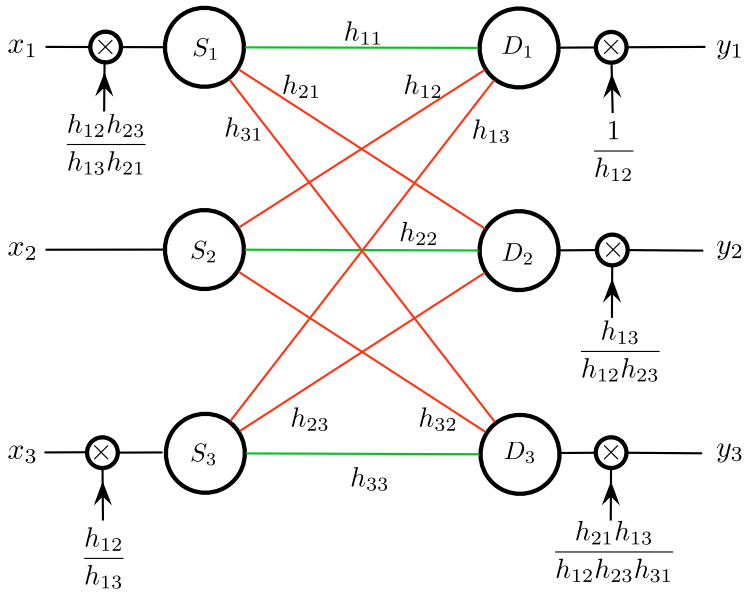

Figure 8: Normalization in 3-user Interference Channel

The normalized 3-user interference channel can be represented as

$$\begin{aligned} y_1 &= \bar{h}_{11}x_1 + x_2 + x_3 \\ y_2 &= x_1 + \bar{h}_{22}x_2 + x_3 \\ y_3 &= x_1 + \bar{h}x_2 + \bar{h}_{33}x_3 \end{aligned}$$

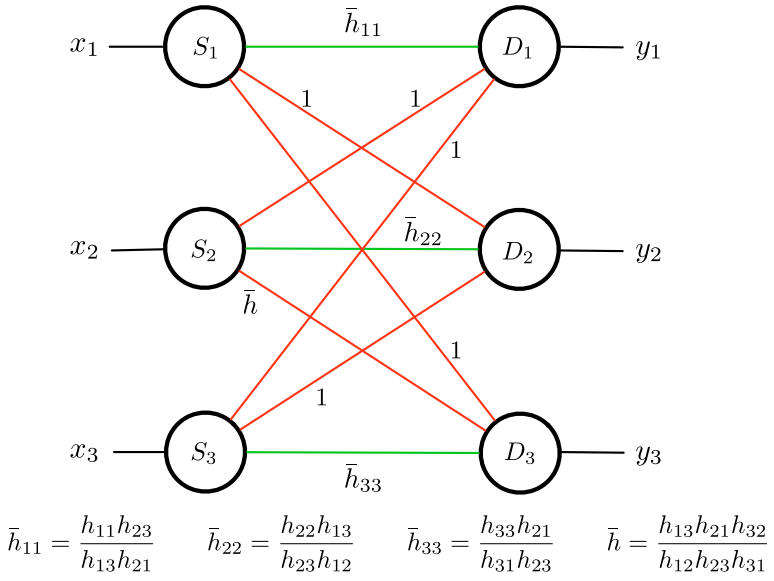

Figure 9: Normalized 3-user Interference Channel

wherein we have reduced channel parameters to four channel coefficients $\bar{h}_{11}, \bar{h}_{22}, \bar{h}_{33}, \bar{h}$, defined as

$$\bar{h}_{11} = \frac{h_{11}h_{23}}{h_{13}h_{21}}, \qquad \bar{h}_{22} = \frac{h_{22}h_{13}}{h_{23}h_{12}}, \qquad \bar{h}_{33} = \frac{h_{33}h_{21}}{h_{31}h_{23}}, \qquad \bar{h} = \frac{h_{13}h_{21}h_{32}}{h_{12}h_{23}h_{31}} \tag{67}$$

All symbols are still over $\mathbb{F}_{p^n}$ and we have the normalized interference channel illustrated in Fig. 9.

3.4 Linear-scheme Capacity of the Finite Field Interference Channel

In the study of the X channel, we noted how scalar channels over $\mathbb{F}_{p^n}$ can be viewed as $n \times n$ MIMO channels over $\mathbb{F}_p$. Let us see if the same insight can be carried over to the 3 user interference channel. For the 3 user MIMO interference channel, an eigenvector based interference alignment solution that achieves the optimal DoF value, is introduced by Cadambe and Jafar in [4]. Let us see if the same solution applies in the finite field setting as well. As we will show, while the eigenvector solution holds in the wireless case for almost all channel realizations, because of channel structure in the finite field case, the solution holds only in certain 'degenerate' settings, that are increasingly rare as the base field size increases, so that in the limit of infinite p, the eigenvector solution does not hold, almost surely.

Theorem 3 *Fully connected 3-user interference channel over $\mathbb{F}_{p^n}$ has capacity $C = C_{linear} = \frac{3}{2}$ for all $p > 3$, if*

$$\bar{h}_{kk} \notin \mathbb{F}_p, k \in \{1, 2, 3\} \tag{68}$$

$$\bar{h} \in \mathbb{F}_p \tag{69}$$

Proof: The outer bound of $\frac{3}{2}$ extends from [4] with only minor adjustments to account for operating over finite fields. Achievable scheme is presented here. Let us denote the $n \times n$ linear transformation corresponding to product by $\bar{h}$ as H. i.e., $\bar{h} \in \mathbb{F}_{p^n}$ and $H \in \mathbb{F}_p^{n \times n}$. The achievable scheme involves beamforming vectors $\bar{V}_1, \bar{V}_2, \bar{V}_3 \in \mathbb{F}_p^{n \times 1}$ at the 3 sources such that interference is aligned at all destinations. Note that we need eigenvectors of H (and also the eigenvalues) to be in $\mathbb{F}_p$. This implies that the eigen vector solution of [4] can be used only when $\bar{h} \in \mathbb{F}_p$ to achieve linear-scheme capacity of $\frac{3}{2}$. Note that this is analogous to the asymmetric complex signaling setting studied in [7] where because the scalar complex channels become rotation matrices over reals, they do not have eigenvectors over reals unless the rotation is identity. Since $\bar{h} \in \mathbb{F}_p$, H is a scaled identity matrix, and every vector is an eigenvector of this matrix. Let us choose the same beamforming matrices at the 3 sources, $\bar{V} = \bar{V}_1 = \bar{V}_2 = \bar{V}_3$. This ensures that interference is aligned at all destinations for the normalized 3-user interference channel. At destination 3, interference from source 2 ($\bar{h}\bar{V}$) spans the same space as interference from source 1 ($\bar{V}$), since $\bar{h} \in \mathbb{F}_p$. Having aligned interference at the destinations, we now discuss construction of the beamforming matrix for odd and even n, such that desired and interference symbols are linearly independent at all destinations.

Achievability for even $n = 2l$:
When n is even ($n = 2l$), we choose $\bar{V} \in \mathbb{F}_{p^n}^{1 \times l}$ and send l input symbols per channel use ($x_1, \ldots, x_l \in \mathbb{F}_p$) from each source. Since $\bar{V} = \bar{V}_1 = \bar{V}_2 = \bar{V}_3$, it can be noted that interference will be aligned at all destinations in l dimensional space. Let us denote the l columns of $\bar{V}$ as $V_1, V_2, \ldots, V_l$. Then, signal space at the three destinations can be represented as

$$S_k = [\bar{h}_{kk}\bar{V} \quad \bar{V}] = [\bar{h}_{kk}V_1, \bar{h}_{kk}V_2, \ldots, \bar{h}_{kk}V_l, \;\; V_1, V_2, \ldots, V_l], \quad k \in \{1, 2, 3\} \tag{70}$$

We now describe how to choose columns of $\bar{V}$ such that desired and interference symbols are linearly independent at all destinations. Let us choose V_1 to be 1. This implies that the 2 columns $[\bar{h}_{kk}V_1 \;\; V_1] = [\bar{h}_{kk} \;\; 1]$ in S_k are linearly independent over $\mathbb{F}_p$ since $\bar{h}_{kk} \notin \mathbb{F}_p, k \in \{1, 2, 3\}$. Now let us construct V_2 such that 4 columns of S_k are linearly independent over $\mathbb{F}_p$ for $k \in \{1, 2, 3\}$.

$$\text{From } S_k, \quad V_2 \notin A_k \;\; \triangleq \;\; \left\{ \frac{(\alpha_1 \bar{h}_{kk} + \alpha_2)V_1}{\beta_1 \bar{h}_{kk} + \beta_2} : \alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}_p, (\beta_1, \beta_2) \neq (0, 0) \right\} \tag{71}$$

Now we note that

$$|A_k| \;\; \leq \;\; \frac{(p^2 - 1)p^2}{p - 1} = p^3 + p^2, k \in \{1, 2, 3\} \tag{72}$$

$$|A_1 \cup A_2 \cup A_3| \;\; \leq \;\; 3(p^3 + p^2) \tag{73}$$

There are p^n choices for V_2, and since $p^n > 3(p^3 + p^2)$ for all $p > 3$, there exist choices for V_2 such that all 3 conditions of (71) hold. Choosing V_2 from those, we note that 4 columns of S_1, S_2, S_3 are linearly independent over $\mathbb{F}_p$. We proceed recursively in a similar manner, for choosing columns $V_3, V_4, \ldots, V_{l-1}$ such that $6, 8, \ldots, 2(l-1)$ columns are linearly independent over $\mathbb{F}_p$ respectively, in all $S_k, k \in \{1, 2, 3\}$.
Let us now discuss the last iteration wherein we choose column V_l such that all $n = 2l$ columns are linearly independent over $\mathbb{F}_p$ in all $S_k, k \in \{1, 2, 3\}$, given that $2l - 2$ columns are already linearly

independent with appropriate choices of $V_1, V_2, \ldots, V_{l-1}$.

$$\text{From } S_k, \quad V_l \notin A_k \triangleq \{\frac{(\alpha_1\bar{h}_{kk}+\alpha_2)V_1+(\alpha_3\bar{h}_{kk}+\alpha_4)V_2+\cdots+(\alpha_{2l-3}\bar{h}_{kk}+\alpha_{2l-2})V_{l-1}}{\beta_1\bar{h}_{kk}+\beta_2}: \\ \alpha_i,\beta_1,\beta_2 \in \mathbb{F}_p, i \in \{1,\ldots,2l-2\}, (\beta_1,\beta_2)\neq(0,0)\} \tag{74}$$

Now we note that

$$|A_k| \leq \frac{(p^2-1)p^{2l-2}}{p-1} = p^{2l-1}+p^{2l-2}, k \in \{1,2,3\} \tag{75}$$

$$|A_1 \cup A_2 \cup A_3| \leq 3(p^{2l-1}+p^{2l-2}) \tag{76}$$

There are $p^n = p^{2l}$ choices for V_l, and since $p^{2l} > 3(p^{2l-1}+p^{2l-2})$ for all $p > 3$, there exist choices for V_l such that all 3 conditions of (74) hold. Choosing V_l from those, we note that all n columns of S_1, S_2, S_3 are linearly independent over $\mathbb{F}_p$. Hence, desired and interference symbols are linearly independent at all destinations. Thus, sum rate of $\frac{3}{2}$ is achieved over $\mathbb{F}_{p^n}$ for all even n with $p > 3$, if $\bar{h}_{kk} \notin \mathbb{F}_p, k \in \{1,2,3\}$ and $\bar{h} \in \mathbb{F}_p$.

Achievability for odd $n = 2l+1$:
Consider a 2 symbol extension of the channel with $2n$ dimensions of order p at each destination. We choose $\bar{V} \in \mathbb{F}_{p^n}^{2\times n}$ and send n input symbols over 2 channel uses ($x_1, \ldots, x_n \in \mathbb{F}_p$) from each source. Interference will be aligned at all destinations in an n dimensional space. The signal space at the three destinations can be represented as

$$S_k = [\bar{h}_{kk}\bar{V} \quad \bar{V}] = [\bar{h}_{kk}V_1, \bar{h}_{kk}V_2, \ldots, \bar{h}_{kk}V_n, \ V_1, V_2, \ldots, V_n], \quad k \in \{1,2,3\} \tag{77}$$

Let us choose V_1 to be vector of ones. This implies that the 2 columns $[\bar{h}_{kk}V_1 \ \ V_1]$ in S_k are linearly independent over $\mathbb{F}_p$ since $\bar{h}_{kk} \notin \mathbb{F}_p, k \in \{1,2,3\}$. Now let us construct V_2 such that 4 columns of S_k are linearly independent over $\mathbb{F}_p$ for $k \in \{1,2,3\}$.

$$\text{From } S_k, \quad V_2 \notin A_k \triangleq \left\{\frac{(\alpha_1\bar{h}_{kk}+\alpha_2)V_1}{\beta_1\bar{h}_{kk}+\beta_2}: \alpha_1,\alpha_2,\beta_1,\beta_2 \in \mathbb{F}_p, (\beta_1,\beta_2)\neq(0,0)\right\} \tag{78}$$

Now we note that

$$|A_k| \leq \frac{(p^2-1)p^2}{p-1} = p^3+p^2, k \in \{1,2,3\} \tag{79}$$

$$|A_1 \cup A_2 \cup A_3| \leq 3(p^3+p^2) \tag{80}$$

There are p^{2n} choices for V_2, and since $p^{2n} > 3(p^3+p^2)$ for all p, there exist choices for V_2 such that all 3 conditions of (78) hold. Choosing V_2 from those, we note that 4 columns of S_1, S_2, S_3 are linearly independent over $\mathbb{F}_p$. We proceed recursively in a similar manner, for choosing columns $V_3, V_4, \ldots, V_{n-1}$ such that $6, 8, \ldots, 2(n-1)$ columns are linearly independent over $\mathbb{F}_p$ respectively, in all $S_k, k \in \{1,2,3\}$.
Let us now discuss the last iteration wherein we choose column V_n such that all n columns are linearly independent over $\mathbb{F}_p$ in all $S_k, k \in \{1,2,3\}$, given that $2n-2$ columns are already linearly

independent with appropriate choices of $V_1, V_2, \ldots, V_{n-1}$.

$$\text{From } S_k, \quad V_n \notin A_k \triangleq \{\frac{(\alpha_1\bar{h}_{kk}+\alpha_2)V_1+(\alpha_3\bar{h}_{kk}+\alpha_4)V_2+\cdots+(\alpha_{2n-3}\bar{h}_{kk}+\alpha_{2n-2})V_{n-1}}{\beta_1\bar{h}_{kk}+\beta_2}: \\ \alpha_i,\beta_1,\beta_2 \in \mathbb{F}_p, i \in \{1,\ldots,2n-2\}, (\beta_1,\beta_2)\neq(0,0)\} \tag{81}$$

Now we note that

$$|A_k| \leq \frac{(p^2-1)p^{2n-2}}{p-1} = p^{2n-1}+p^{2n-2}, k \in \{1,2,3\} \tag{82}$$

$$|A_1 \cup A_2 \cup A_3| \leq 3(p^{2n-1}+p^{2n-2}) \tag{83}$$

There are p^{2n} choices for V_l, and since $p^{2n} > 3(p^{2n-1}+p^{2n-2})$ for all $p > 3$, there exist choices for V_n such that all 3 conditions of (81) hold. Choosing V_n from those, we note that all n columns of S_1, S_2, S_3 are linearly independent over $\mathbb{F}_p$. Hence, desired and interference symbols are linearly independent at all destinations. Thus, sum rate of $\frac{3}{2}$ is achieved over $\mathbb{F}_{p^n}$ for all odd n with $p > 3$, if $\bar{h}_{kk} \notin \mathbb{F}_p, k \in \{1,2,3\}$ and $\bar{h} \in \mathbb{F}_p$.

The fraction of channel realizations for which the conditions $\bar{h}_{kk} \notin \mathbb{F}_p, k \in \{1,2,3\}$ and $\bar{h} \in \mathbb{F}_p$ hold, is given by

$$\frac{p}{p^n} \times (\frac{p^n-p}{p^n})^3. \tag{84}$$

which goes to 0 as $p \to \infty$. ■

The implications of the structure of the channel become evident now. While we have $n \times n$ MIMO channels, they behave like channels with diversity n, e.g, like diagonal channels, where also the eigenvector solution does not work except over a measure 0 set. To strengthen this insight, we explore the 3-user interference channel further.

3.4.1 Insight: Channel Diversity

As noted for X networks earlier, the finite field $\mathbb{F}_{p^n}$ is analogous to a $n \times n$ MIMO network with special channel structure. The main insight that arises out of exploring the 3-user interference channel is that *n is analogous to channel diversity.* This is similar to saying that a scalar channel over $\mathbb{F}_{p^n}$ is analogous to n parallel channels over $\mathbb{F}_p$. In the remainder of this work, we will focus only on linear capacity C_{linear} and reinforce the parallels between n and channel diversity.

3.4.2 Main Result

It is known from [29] that the 3-user interference channel over $\mathbb{F}_{p^n}$ has channel diversity n, and so has linear capacity of $\frac{3D}{2D+1}$ when using linear beam forming schemes with alignment depth $D = 2n - \lfloor n/2 \rfloor - 1$. The alignment depth, i.e., the length of the longest chain of one-to-one alignments, which is a function of channel diversity, is the primary limiting factor impacting both achievability and converse arguments. The achievable scheme is essentially the asymptotic interference alignment scheme of [4]. Outer bounds for linear schemes come from the argument that that the alignment depth cannot be more than D, and suppose it were, then desired signal would lie in span of the interference signal at the receivers. The result translates into the finite field setting as follows. We will focus mainly on the case where n is odd (the cases where n is even follow similarly and will be touched upon briefly).

Theorem 4 *The 3-user interference channel over $\mathbb{F}_{p^n}$ with odd $n = 2l+1$ has linear capacity $C_{linear} = \frac{3l+1}{2l+1}$ if*

$$\bar{h}_{11} \notin A \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_{l-1}\bar{h}^{l-1}}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_l\bar{h}^l} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \right\} \quad (85)$$

$$\bar{h}_{22} \notin B \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_l\bar{h}^l}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_{l-1}\bar{h}^{l-1}} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_{l-1}) \neq (0, \ldots, 0) \right\} \quad (86)$$

$$\bar{h}_{33} \notin C \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_l\bar{h}^l}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_{l-1}\bar{h}^{l-1}} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_{l-1}) \neq (0, \ldots, 0) \right\} \quad (87)$$

$$\beta_l\bar{h}^l + \ldots + \beta_1\bar{h} + \beta_0 \neq 0 : \beta_0, \ldots, \beta_l \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \quad (88)$$

The outer bound on linear capacity is presented in Section 3.6. The achievable scheme is presented next.

3.5 Achievability

Over $\mathbb{F}_{p^{2l+1}}$, we will show that $3l+1$ symbols can be transmitted ($l+1$ symbols from source 1 and l symbols each from sources 2 and 3), and all desired symbols are resolvable at the destinations. Symbol extensions will not be necessary here. Note that $\bar{h}$ is equivalent to the T matrix used in the CJ scheme [4], since beamforming directions are identified with varying powers of $\bar{h}$.

We will first discuss the achievable scheme over $\mathbb{F}_{p^3}$ and then show how it extends to all odd n, $\mathbb{F}_{p^{2l+1}}$.

3.5.1 Achievability over $\mathbb{F}_{p^3}$

Proof: Let us consider the normalized 3-user interference channel over $\mathbb{F}_{p^3}$ so that $\bar{h}_{11}, \bar{h}_{22}, \bar{h}_{33}, \bar{h} \in \mathbb{F}_{p^3}$. We will show that linear schemes can achieve the rate of $\frac{4}{3}$. Consider the finite field network wherein source 1 sends 2 symbols, $x_1^1, x_1^2 \in \mathbb{F}_p$, while sources 2 and 3 send only one symbol each, $x_2, x_3 \in \mathbb{F}_p$.

Because of the channel normalization, we use the same beamforming direction $v \in \mathbb{F}_{p^3}$ for symbols sent by sources 2 and 3, so that interference is aligned at destination 1 ($v_2 = v_3 = v$). At source 1, we use 2 beam forming directions $\bar{h}v$ and v so that, one symbol aligns at destination 2, and another aligns at destination 3 ($v_1^1 = v, v_1^2 = \bar{h}v$). With these choices for beamforming directions, the received symbols can be represented as

$$\begin{aligned} y_1 &= \bar{h}_{11}(vx_1^1 + \bar{h}vx_1^2) + vx_2 + vx_3 \\ y_2 &= vx_1^1 + \bar{h}vx_1^2 + \bar{h}_{22}vx_2 + vx_3 \\ y_3 &= vx_1^1 + \bar{h}vx_1^2 + \bar{h}vx_2 + \bar{h}_{33}vx_3 \end{aligned}$$

Note that interference is aligned along v at destinations 1 and 2, while interference at destination 3 is aligned along $\bar{h}v$. There is additional unaligned interference at destinations 2 and 3, but they both have only a single input symbol to be decoded. We have 3 dimensions at each destination over $\mathbb{F}_p$, within which desired and interference symbols need to be resolved. In order to resolve desired symbols at the destinations, the signal spaces containing desired and interference symbols need to

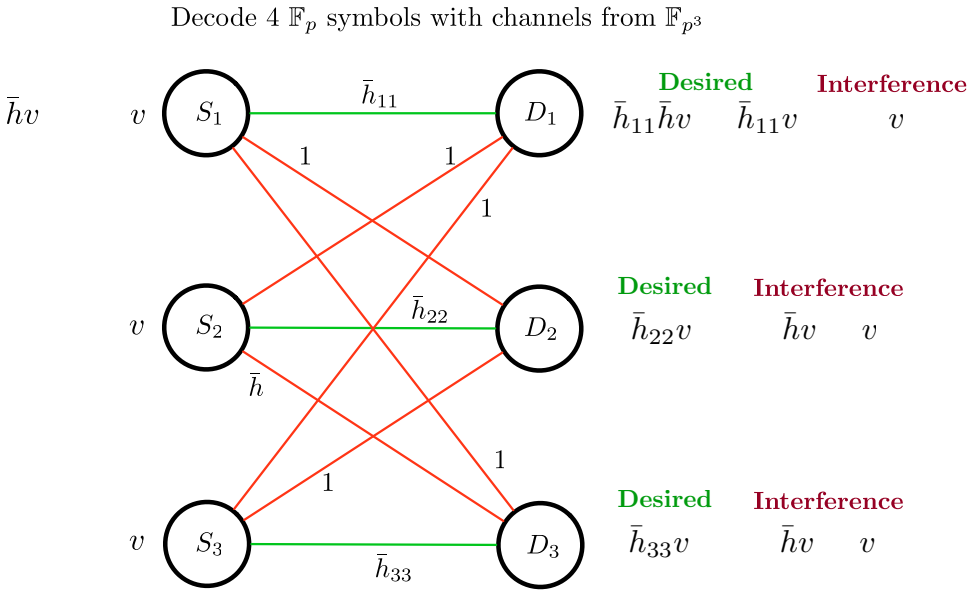

Figure 10: 3-user Interference channel over $\mathbb{F}_{p^3}$

have linearly independent elements.

$$S_1 = [\bar{h}_{11}\bar{h}v \quad \bar{h}_{11}v \quad v] = \bar{h}_{11}[\bar{h} \quad 1 \quad \frac{1}{\bar{h}_{11}}]v \tag{89}$$

$$S_2 = [\bar{h}_{22}v \quad \bar{h}v \quad v] = [\bar{h}_{22} \quad \bar{h} \quad 1]v \tag{90}$$

$$S_3 = [\bar{h}_{33}v \quad \bar{h}v \quad v] = [\bar{h}_{33} \quad \bar{h} \quad 1]v \tag{91}$$

When $\bar{h} \notin \mathbb{F}_p$, $\bar{h}$ and 1 are linearly independent over $\mathbb{F}_p$. Hence, elements of S_1 can be linearly dependent only if $\frac{1}{\bar{h}_{11}}$ is a linear combination of $\bar{h}$ and 1. Similarly elements of S_2 and S_3 can be linearly dependent only if $\bar{h}_{22}$ or $\bar{h}_{33}$ is a linear combination of $\bar{h}$ and 1, respectively. Thus, the scheme works when the following conditions are satisfied.

$$\bar{h}_{11} \notin A \triangleq \left\{ \frac{1}{\beta_0 + \beta_1 \bar{h}} : \beta_0, \beta_1 \in \mathbb{F}_p, (\beta_0, \beta_1) \neq (0,0) \right\} \cup \{0\} \tag{92}$$

$$\bar{h}_{22} \notin B \triangleq \{\alpha_0 + \alpha_1 \bar{h} : \alpha_0, \alpha_1 \in \mathbb{F}_p\} \tag{93}$$

$$\bar{h}_{33} \notin C \triangleq \{\alpha_0 + \alpha_1 \bar{h} : \alpha_0, \alpha_1 \in \mathbb{F}_p\} \tag{94}$$

$$\bar{h} \notin \mathbb{F}_p \tag{95}$$

Hence we can achieve the rate of 4 $\mathbb{F}_p$ symbols per channel use, i.e., $\frac{4}{3}$ $\mathbb{F}_{p^3}$ symbols per channel use. Fig. 10 illustrates the achievable scheme described for $\mathbb{F}_{p^3}$. ■

Remark 1: We can rewrite the conditions in terms of original channel coefficients as follows.

$$\frac{1}{h_{11}} \notin A \triangleq \left\{ \alpha_1 \frac{h_{32}}{h_{12}h_{31}} + \beta_1 \frac{h_{23}}{h_{13}h_{21}} : \alpha_1, \beta_1 \in \mathbb{F}_p \right\} \quad (96)$$

$$h_{22} \notin B \triangleq \left\{ \alpha_2 \frac{h_{21}h_{32}}{h_{31}} + \beta_2 \frac{h_{12}h_{23}}{h_{13}} : \alpha_2, \beta_2 \in \mathbb{F}_p \right\} \quad (97)$$

$$h_{33} \notin C \triangleq \left\{ \alpha_3 \frac{h_{13}h_{32}}{h_{12}} + \beta_3 \frac{h_{31}h_{23}}{h_{21}} : \alpha_3, \beta_3 \in \mathbb{F}_p \right\} \quad (98)$$

These conditions, which are obtained for the constant channel setting, are similar to the conditions for feasibility of PBNA derived in [2] for the time-varying setting, wherein 6 cofactors of off-diagonal channel coefficients are involved in the feasibility criteria. However, note that in this finite field channel, the combining coefficients $\alpha_k, \beta_k, k \in \{1, 2, 3\}$ can be from $\mathbb{F}_p$ whereas in [2], only binary coefficients were involved.

Remark 2: Each of the direct channels h_{ii} can take one of p^3 values. At most p^2 of these can be linear combination of the cross channel functions. Hence, there are at least $p^3 - p^2$ choices for each direct channel such that the linear independence conditions are met and so desired symbols are resolvable. The fraction of channel realizations for which h_{ii} is not a linear combination of cross channel functions, is therefore at least

$$\frac{p^3 - p^2}{p^3} = 1 - \frac{1}{p} \to 1 \text{ for large } p. \quad (99)$$

The fraction of channels for which the scheme works, considering all conditions simultaneously is therefore at least

$$(\frac{p^3 - p}{p^3}) \times (1 - \frac{1}{p})^3 = (1 - \frac{1}{p^2}) \times (1 - \frac{1}{p})^3 \to 1 \text{ for large } p.$$

Note that unlike the wireless case where the DoF results are proved in an almost surely sense, the guarantee on the fraction of channels for which the scheme works is much more interesting.

3.5.2 Achievability over $\mathbb{F}_{p^n}$, $n = 2l + 1$

Proof: Now let us show that the sum-rate of $\frac{3l+1}{2l+1}$ can be achieved over $\mathbb{F}_{p^{2l+1}}$, which generalizes the proof for $\mathbb{F}_{p^3}$ discussed earlier, to any odd n. Suppose source 1 sends $l+1$ symbols, $x_1^1, x_1^2, \ldots x_1^{l+1} \in \mathbb{F}_p$, while sources 2 and 3 sends l symbols each, $x_2^1, \ldots, x_2^l, x_3^1, \ldots, x_3^l \in \mathbb{F}_p$.

We use the same set of beamforming directions, $\bar{h}^{l-1}v, \ldots, \bar{h}v, v$ with $v \in \mathbb{F}_{p^{2l+1}}$ for the l symbols sent by sources 2 and 3, so that interference is aligned at destination 1 in span($[\bar{h}^{l-1}v \ \ldots \ \bar{h}v \ v]$). At source 1, we use $l+1$ beamforming directions $\bar{h}^l v, \ldots, \bar{h}v, v$ so that, l symbols align at destination 2, and l symbols align at destination 3. With these choices of beamforming directions for input symbols, the received symbols at the destinations can be represented as

$$\begin{aligned}
y_1 &= \bar{h}_{11}(\bar{h}^l v x_1^{l+1} + \ldots + \bar{h}v x_1^2 + v x_1^1) + \bar{h}^{l-1} v x_2^l + \ldots + v x_2^1 + \bar{h}^{l-1} v x_3^l + \ldots + v x_3^1 \\
y_2 &= \bar{h}^l v x_1^{l+1} + \ldots + \bar{h}v x_1^2 + v x_1^1 + \bar{h}_{22}\bar{h}^{l-1} v x_2^l + \ldots + \bar{h}_{22} v x_2^1 + \bar{h}^{l-1} v x_3^l + \ldots + v x_3^1 \\
y_3 &= \bar{h}^l v x_1^{l+1} + \ldots + \bar{h}v x_1^2 + v x_1^1 + \bar{h}^{l-1} v x_2^l + \ldots + v x_2^1 + \bar{h}_{33}\bar{h}^{l-1} v x_3^l + \ldots + \bar{h}_{33} v x_3^1
\end{aligned}$$

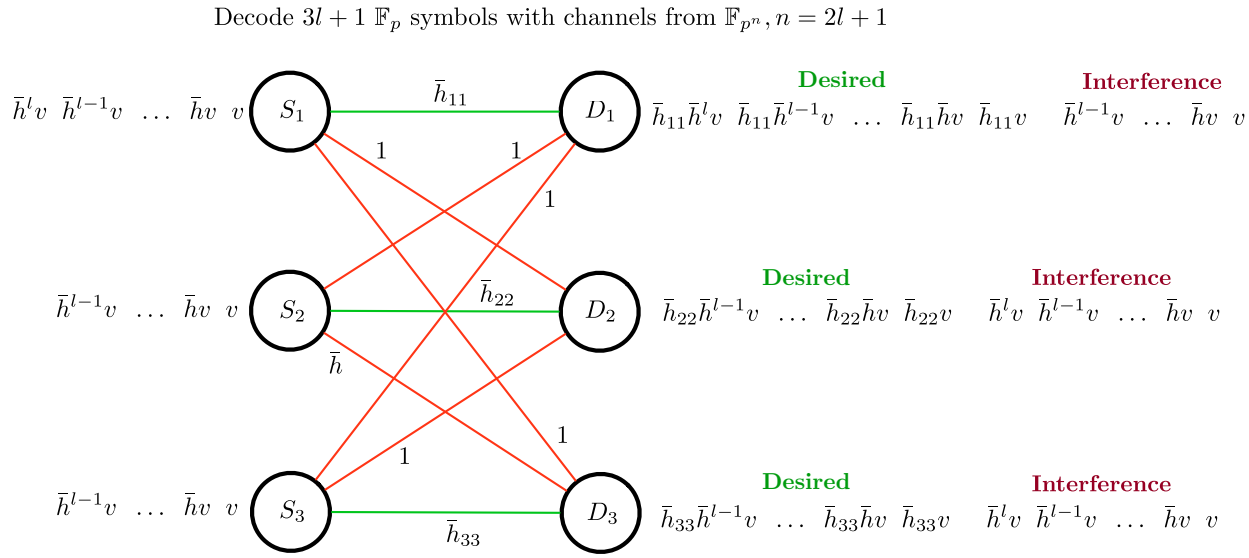

Figure 11: 3-user Interference channel over $\mathbb{F}_{p^n}$, $n = 2l+1$

In order to resolve desired symbols at the destinations, signal spaces containing desired and interference symbols need to have linearly independent entries.

$$S_1 = [\bar{h}_{11}\bar{h}^l v \ \ldots \ \bar{h}_{11}\bar{h} v \ \bar{h}_{11} v \ \bar{h}^{l-1} v \ \ldots \ \bar{h} v \ v] = [\bar{h}_{11}\bar{h}^l \ \ldots \ \bar{h}_{11}\bar{h} \ \bar{h}_{11} \ \bar{h}^{l-1} \ \ldots \ \bar{h} \ 1]v \quad (100)$$

$$S_2 = [\bar{h}_{22}\bar{h}^{l-1} v \ \ldots \ \bar{h}_{22}\bar{h} v \ \bar{h}_{22} v \ \bar{h}^l v \ \ldots \ \bar{h} v \ v] = [\bar{h}_{22}\bar{h}^{l-1} \ \ldots \ \bar{h}_{22}\bar{h} \ \bar{h}_{22} \ \bar{h}^l \ \ldots \ \bar{h} \ 1]v \quad (101)$$

$$S_3 = [\bar{h}_{33}\bar{h}^{l-1} v \ \ldots \ \bar{h}_{33}\bar{h} v \ \bar{h}_{33} v \ \bar{h}^l v \ \ldots \ \bar{h} v \ v] = [\bar{h}_{33}\bar{h}^{l-1} \ \ldots \ \bar{h}_{33}\bar{h} \ \bar{h}_{33} \ \bar{h}^l \ \ldots \ \bar{h} \ 1]v \quad (102)$$

The desired and interference symbols are resolvable and $3l+1$ symbols can be decoded at the destinations when the foliowing conditions are satisfied.

$$\bar{h}_{11} \notin A \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_{l-1}\bar{h}^{l-1}}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_l\bar{h}^l} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \right\} \quad (103)$$

$$\bar{h}_{22} \notin B \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_l\bar{h}^l}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_{l-1}\bar{h}^{l-1}} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_{l-1}) \neq (0, \ldots, 0) \right\} \quad (104)$$

$$\bar{h}_{33} \notin C \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_l\bar{h}^l}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_{l-1}\bar{h}^{l-1}} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_{l-1}) \neq (0, \ldots, 0) \right\} \quad (105)$$

$$\beta_l\bar{h}^l + \ldots + \beta_1\bar{h} + \beta_0 \neq 0 : \beta_0, \ldots, \beta_l \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \quad (106)$$

Fig. 11 illustrates the achievable scheme described for $\mathbb{F}_{p^n}$ with $n = 2l+1$. Note that a $\mathbb{F}_p$ symbol represents $\frac{1}{2l+1}$ of an $\mathbb{F}_{p^{2l+1}}$ symbol and rate is measured in $\mathbb{F}_{p^{2l+1}}$ units. Hence we have proved achievability of linear capacity of $\frac{3l+1}{2l+1}$ for all odd $n = 2l+1$. ■

Remark 3: Each of the direct channels h_{ii} can be from one of the p^{2l+1} choices. The fraction of channel realizations for which direct channels satisfy the conditions is at least

$$\text{Fraction of channels with } h_{11} \text{ not in A} \geq \frac{p^{2l+1} - (p^{2l} + \ldots + p^l)}{p^{2l+1}}$$
$$= 1 - \{\frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^{l+1}}\} \to 1 \text{ for large } p. \tag{107}$$

$$\text{Fraction of channels with } h_{22} \text{ or } h_{33} \text{ not in B or C} = \frac{p^{2l+1} - (p^{2l} + \ldots + p^{l+1})}{p^{2l+1}}$$
$$= 1 - \{\frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^l}\} \to 1 \text{ for large } p. \tag{108}$$

Also, following condition on cross channel $\bar{h}$ needs to be met

$$\beta_l \bar{h}^l + \ldots + \beta_1 \bar{h} + \beta_0 \neq 0 : \beta_0, \ldots, \beta_l \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \tag{109}$$

The $l+1$ combining coefficients can repesent no more than p^{l+1} distinct polynomials, and since each has degree l or less, each polynomial can have at most l zeros. Therefore, the number of possible $\bar{h}$ that can violate (109) is no more than lp^{l+1}. So, the fraction of $\bar{h}$ values for which the scheme works is at least

$$\frac{p^{2l+1} - lp^{l+1}}{p^{2l+1}} \quad = \quad 1 - \frac{l}{p^l} \tag{110}$$

which approaches 1 as either p or l approaches infinity. Putting everything together, the fraction of all channels for which the scheme works is at least

$$(1 - \frac{l}{p^l})(1 - \{\frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^{l+1}}\})(1 - \{\frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^l}\})^2 \to 1 \text{ for large } p \tag{111}$$

Remark 4: Using Lemma 2 in Appendix I, the condition on the cross channel in Theorem 4 can be simplified as $\bar{h} \notin \mathbb{F}_p$ for all prime n, since

$$\beta_l \bar{h}^l + \ldots + \beta_1 \bar{h} + \beta_0 \neq 0 \iff \bar{h} \notin \mathbb{F}_p \tag{112}$$

So fraction of channel values for which scheme works with n being prime, is at least

$$(1 - \frac{1}{p^{2l}})(1 - \{\frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^{l+1}}\})(1 - \{\frac{1}{p} + \frac{1}{p^2} + \ldots + \frac{1}{p^l}\})^2 \to 1 \text{ for large } p. \tag{113}$$

3.5.3 Achievability over $\mathbb{F}_{p^2}$

Having established the achievability proof over $\mathbb{F}_{p^n}$ for odd n, we will omit the general case of even n, except to mention that it can be translated from [29] using the same principles as illustrated for odd n and does not offer new insights. However, we will present the achievability proof for the case of $n = 2$ because the corresponding result in [7] uses the asymmetric complex signaling approach which may be of interest. As before, $\mathbb{F}_{p^2}$ can be viewed as a 2-dimensional vector space over subfield $\mathbb{F}_p$, much like the field of complex numbers can be viewed as a 2-dimensional vector space over reals, so that an achievable scheme similar to asymmetric complex signaling of [7] can be used. Hence, we translate the DoF result of [7] into the finite field setting as follows.

Theorem 5 *The 3-user interference channel over $\mathbb{F}_{p^2}$ has linear capacity, $C_{linear} = \frac{6}{5}$, if*

$$\bar{h}_{11} = \frac{h_{11}h_{23}}{h_{13}h_{21}} \notin \mathbb{F}_p, \qquad \bar{h}\bar{h}_{11} = \frac{h_{11}h_{32}}{h_{12}h_{31}} \notin \mathbb{F}_p$$
$$\bar{h}_{22} = \frac{h_{22}h_{13}}{h_{23}h_{12}} \notin \mathbb{F}_p, \qquad \frac{\bar{h}}{\bar{h}_{22}} = \frac{h_{21}h_{32}}{h_{22}h_{31}} \notin \mathbb{F}_p$$
$$\bar{h}_{33} = \frac{h_{33}h_{21}}{h_{31}h_{23}} \notin \mathbb{F}_p, \qquad \frac{\bar{h}}{\bar{h}_{33}} = \frac{h_{32}h_{13}}{h_{33}h_{12}} \notin \mathbb{F}_p$$

Proof: The outer bound follows from [7] in much the same fashion as the outer bound for the previous section follows from [29]. Here we present only the achievability proof. Consider a 5 symbol extension of the normalized 3-user interference channel over $\mathbb{F}_{p^2}$. Over this 5 symbol extensions, 4 input symbols denoted by $x_k^1, x_k^2, x_k^3, x_k^4$ are precoded and transmitted at source k. Each input symbol $x_k^i, i \in \{1,2,3,4\}, k \in \{1,2,3\}$ is from $\mathbb{F}_p$. Corresponding 5×1 beam forming vectors are denoted using vectors $V_k^1, V_k^2, V_k^3, V_k^4 \in \mathbb{F}_{p^2}^{5\times 1}, k \in \{1,2,3\}$. Each destination has 10 dimensions of order p over the symbol extended channel. Desired symbols from corresponding source would occupy 4 dimensions and for resolvability, interference need to occupy only 6 dimensions of order p. Hence at each destination, two of the 8 interference vectors from 2 unintended sources, need to be aligned. To this end, we make the following choices for certain beam forming vectors.

$$V_1^3 = \bar{h}V_2^1, \qquad V_1^4 = V_3^2, \qquad V_2^3 = V_3^1, \qquad V_2^4 = \frac{1}{\bar{h}}V_1^2, \qquad V_3^3 = V_1^1, \qquad V_3^4 = V_2^2 \tag{114}$$

Desired and Interference signal space at the destinations can now be represented as follows.

$$S_1 = [\bar{h}_{11}V_1^1 \;\; \bar{h}_{11}V_1^2 \;\; \bar{h}_{11}V_1^3 \;\; \bar{h}_{11}V_1^4 \;\; V_2^1 \;\; V_2^2 \;\; V_2^3 \;\; V_2^4 \;\; V_3^2 \;\; V_3^3] \tag{115}$$
$$S_2 = [\bar{h}_{22}V_2^1 \;\; \bar{h}_{22}V_2^2 \;\; \bar{h}_{22}V_2^3 \;\; \bar{h}_{22}V_2^4 \;\; V_3^1 \;\; V_3^2 \;\; V_3^3 \;\; V_3^4 \;\; V_1^2 \;\; V_1^3] \tag{116}$$
$$S_3 = [\bar{h}_{33}V_3^1 \;\; \bar{h}_{33}V_3^2 \;\; \bar{h}_{33}V_3^3 \;\; \bar{h}_{33}V_3^4 \;\; V_1^1 \;\; V_1^2 \;\; V_1^3 \;\; V_1^4 \;\; \bar{h}V_2^2 \;\; \bar{h}V_2^3] \tag{117}$$

Due to interference alignment, these matrices can be equivalently re-written as

$$S_1 = [\bar{h}_{11}V_1^1 \;\; \bar{h}_{11}V_1^2 \;\; \bar{h}_{11}\bar{h}V_2^1 \;\; \bar{h}_{11}V_3^2 \;\; V_2^1 \;\; V_2^2 \;\; V_3^1 \;\; \frac{1}{\bar{h}}V_1^2 \;\; V_3^2 \;\; V_1^1] \tag{118}$$
$$S_2 = [\bar{h}_{22}V_2^1 \;\; \bar{h}_{22}V_2^2 \;\; \bar{h}_{22}V_3^1 \;\; \frac{\bar{h}_{22}}{\bar{h}}V_1^2 \;\; V_3^1 \;\; V_3^2 \;\; V_1^1 \;\; V_2^2 \;\; V_1^2 \;\; \bar{h}V_2^1] \tag{119}$$
$$S_3 = [\bar{h}_{33}V_3^1 \;\; \bar{h}_{33}V_3^2 \;\; \bar{h}_{33}V_1^1 \;\; \bar{h}_{33}V_2^2 \;\; V_1^1 \;\; V_1^2 \;\; \bar{h}V_2^1 \;\; V_3^2 \;\; \bar{h}V_2^2 \;\; \bar{h}V_3^1] \tag{120}$$

In order to resolve desired signals at all destinations, the columns of these 3 matrices need to be linearly independent over $\mathbb{F}_p$. The following six conditions are required.

$$\bar{h}_{11} \notin \mathbb{F}_p, \qquad \bar{h}\bar{h}_{11} \notin \mathbb{F}_p, \qquad \bar{h}_{22} \notin \mathbb{F}_p, \qquad \frac{\bar{h}}{\bar{h}_{22}} \notin \mathbb{F}_p, \qquad \bar{h}_{33} \notin \mathbb{F}_p, \qquad \frac{\bar{h}}{\bar{h}_{33}} \notin \mathbb{F}_p$$

We will now choose beam forming vectors $V_k^i, i \in \{1,2\}, k \in \{1,2,3\}$, such that all three matrices S_k have their 10 columns linearly independent.

We choose V_1^1 to be the vector of ones. Since $\bar{h}_{11}, \bar{h}_{33} \notin \mathbb{F}_p$, vectors in $S_1 : [\bar{h}_{11}V_1^1 \;\; V_1^1]$ are linearly independent and so are similar vectors in $S_3 : [\bar{h}_{33}V_1^1 \;\; V_1^1]$. We now choose vector V_1^2 such that following conditions hold.

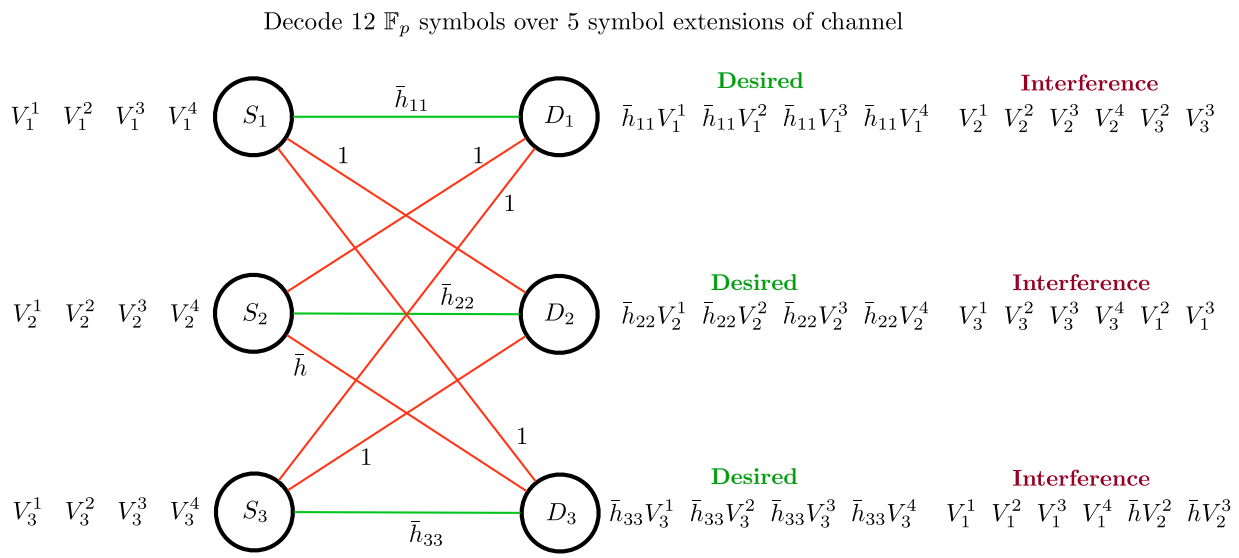

Figure 12: 3-user Interference channel over $\mathbb{F}_{p^2}$

$$\text{From } S_1,\ V_1^2 \notin A \ \triangleq\ \left\{ \frac{(\alpha_1\bar{h}_{11}+\alpha_2)V_1^1}{\beta_1\bar{h}_{11}+\beta_2\frac{1}{\bar{h}}} : \alpha_1,\alpha_2,\beta_1,\beta_2 \in \mathbb{F}_p, (\beta_1,\beta_2)\neq(0,0) \right\} \tag{121}$$

$$\text{From } S_2,\ V_1^2 \notin B \ \triangleq\ \left\{ \frac{\alpha_1 V_1^1}{\beta_1+\beta_2\frac{\bar{h}_{22}}{\bar{h}}} : \alpha_1,\beta_1,\beta_2 \in \mathbb{F}_p, (\beta_1,\beta_2)\neq(0,0) \right\} \tag{122}$$

$$\text{From } S_3,\ V_1^2 \notin C \ \triangleq\ \left\{(\alpha_1\bar{h}_{33}+\alpha_2)V_1^1 : \alpha_1,\alpha_2 \in \mathbb{F}_p\right\} \tag{123}$$

Now we note that

$$|A| \le \frac{(p^2-1)p^2}{p-1} = p^3+p^2, \qquad |B| \le \frac{(p^2-1)p}{p-1} = p^2+p, \qquad |C| \le p^2 \tag{124}$$

$$|A\cup B\cup C| \le p^3+3p^2+p \tag{125}$$

There are p^{10} choices for $V_1^2 \in \mathbb{F}_{p^2}^{5\times 1}$, and since

$$p^{10} \ > \ p^3+3p^2+p \tag{126}$$

for all p, there exist choices for V_1^2 such that all 3 conditions (121),(122),(123) hold. Choosing V_1^2 from those, we note that 4 columns of S_1 and 3 columns each of S_2, S_3 are linearly independent over $\mathbb{F}_p$.

Now we choose V_2^1 similarly such that following conditions hold

$$V_2^1 \notin A \triangleq \{\frac{(\alpha_1\bar{h}_{11}+\alpha_2)V_1^1+(\alpha_3\bar{h}_{11}+\frac{1}{\bar{h}}\alpha_4)V_1^2}{\beta_1\bar{h}_{11}\bar{h}+\beta_2} : \alpha_1,\alpha_2,\alpha_3,\alpha_4,\beta_1,\beta_2 \in \mathbb{F}_p, (\beta_1,\beta_2)\neq(0,0)\} \tag{127}$$

$$V_2^1 \notin B \triangleq \{\frac{\alpha_1 V_1^1+(\alpha_2+\alpha_3\frac{\bar{h}_{22}}{\bar{h}})V_1^2}{\beta_1\bar{h}_{22}+\beta_2\bar{h}} : \alpha_1,\alpha_2,\alpha_3,\beta_1,\beta_2 \in \mathbb{F}_p, (\beta_1,\beta_2)\neq(0,0)\} \tag{128}$$

$$V_2^1 \notin C \triangleq \{\frac{(\alpha_1\bar{h}_{33}+\alpha_2)V_1^1+\alpha_3 V_1^2}{\bar{h}} : \alpha_1,\alpha_2,\alpha_3 \in \mathbb{F}_p\} \tag{129}$$

Now we note that

$$|A| \leq \frac{(p^2-1)p^4}{p-1} = p^5+p^4, \qquad |B| \leq \frac{(p^2-1)p^3}{p-1} = p^4+p^3, \qquad |C| \leq p^3 \tag{130}$$

$$|A\cup B\cup C| \leq p^5+2p^4+2p^3 \tag{131}$$

There are p^{10} choices for V_2^1, and since

$$p^{10} \quad > \quad p^5+2p^4+2p^3 \tag{132}$$

for all p, there exist choices for V_2^1 such that all 3 conditions (127),(128),(129) hold. Choosing V_2^1 from those, we note that 6 columns of S_1, 5 columns of S_2 and 4 columns of S_3 are linearly independent over $\mathbb{F}_p$.

Now we choose V_2^2 similarly such that following conditions hold

$$V_2^2 \notin A \triangleq \{(\alpha_1\bar{h}_{11}+\alpha_2)V_1^1+(\alpha_3\bar{h}_{11}+\frac{1}{\bar{h}}\alpha_4)V_1^2+(\alpha_5\bar{h}_{11}\bar{h}+\alpha_6)V_2^1 : \alpha_k \in \mathbb{F}_p, k\in\{1,\ldots,6\}\} \tag{133}$$

$$V_2^2 \notin B \triangleq \{\frac{\alpha_1 V_1^1+(\alpha_2+\alpha_3\frac{\bar{h}_{22}}{\bar{h}})V_1^2+(\alpha_4\bar{h}+\alpha_5\bar{h}_{22})V_2^1}{\beta_1\bar{h}_{22}+\beta_2} : \alpha_k,\beta_1,\beta_2 \in \mathbb{F}_p, k\in\{1,\ldots,5\}, (\beta_1,\beta_2)\neq(0,0)\} \tag{134}$$

$$V_2^2 \notin C \triangleq \{\frac{(\alpha_1\bar{h}_{33}+\alpha_2)V_1^1+\alpha_3 V_1^2+\alpha_4\bar{h}V_2^1}{\beta_1\bar{h}_{33}+\beta_2\bar{h}} : \alpha_k,\beta_1,\beta_2 \in \mathbb{F}_p, k\in\{1,\ldots,4\}, (\beta_1,\beta_2)\neq(0,0)\} \tag{135}$$

Now we note that

$$|A| \leq p^6, \qquad |B| \leq \frac{(p^2-1)p^5}{p-1} = p^6+p^5, \qquad |C| \leq \frac{(p^2-1)p^4}{p-1} = p^5+p^4 \tag{136}$$

$$|A\cup B\cup C| \leq 2p^6+2p^5+p^4 \tag{137}$$

There are p^{10} choices for V_2^2, and since

$$p^{10} \quad > \quad 2p^6 + 2p^5 + p^4 \tag{138}$$

for all p, there exist choices for V_2^2 such that all 3 conditions (133),(134),(135) hold. Choosing V_2^2 from those, we note that 7 columns each of S_1, S_2, and 6 columns of S_3 are linearly independent over $\mathbb{F}_p$.

Now we choose V_3^1 similarly such that following conditions hold

$$\begin{aligned} V_3^1 \notin A \triangleq &\{(\alpha_1\bar{h}_{11} + \alpha_2)V_1^1 + (\alpha_3\bar{h}_{11} + \frac{1}{\bar{h}}\alpha_4)V_1^2 + (\alpha_5\bar{h}_{11}\bar{h} + \alpha_6)V_2^1 + \alpha_7 V_2^2 : \\ &\alpha_k \in \mathbb{F}_p, k \in \{1, \ldots, 7\}\} \end{aligned} \tag{139}$$

$$\begin{aligned} V_3^1 \notin B \triangleq &\{\frac{\alpha_1 V_1^1 + (\alpha_2 + \alpha_3\frac{\bar{h}_{22}}{\bar{h}})V_1^2 + (\alpha_4\bar{h} + \alpha_5\bar{h}_{22})V_2^1 + (\alpha_6\bar{h}_{22} + \alpha_7)V_2^2}{\beta_1\bar{h}_{22} + \beta_2} : \\ &\alpha_k, \beta_1, \beta_2 \in \mathbb{F}_p, k \in \{1, \ldots, 7\}, (\beta_1, \beta_2) \neq (0, 0)\} \end{aligned} \tag{140}$$

$$\begin{aligned} V_3^1 \notin C \triangleq &\{\frac{(\alpha_1\bar{h}_{33} + \alpha_2)V_1^1 + \alpha_3 V_1^2 + \alpha_4\bar{h}V_2^1 + (\alpha_5\bar{h}_{33} + \alpha_6\bar{h})V_2^2}{\beta_1\bar{h}_{33} + \beta_2\bar{h}} : \\ &\alpha_k, \beta_1, \beta_2 \in \mathbb{F}_p, k \in \{1, \ldots, 6\}, (\beta_1, \beta_2) \neq (0, 0)\} \end{aligned} \tag{141}$$

Now we note that

$$|A| \leq p^7, \qquad |B| \leq \frac{(p^2-1)p^7}{p-1} = p^8 + p^7, \qquad |C| \leq \frac{(p^2-1)p^6}{p-1} = p^7 + p^6 \tag{142}$$

$$|A \cup B \cup C| \leq p^8 + 3p^7 + p^6 \tag{143}$$

There are p^{10} choices for V_3^1, and since

$$p^{10} \quad > \quad p^8 + 3p^7 + p^6 \tag{144}$$

for all p, there exist choices for V_3^1 such that all 3 conditions (139),(140),(141) hold. Choosing V_3^1 from those, we note that 8 columns each of S_1, S_3, and 9 columns of S_2 are linearly independent over $\mathbb{F}_p$.

Now we choose V_3^2 similarly such that following conditions hold

$$\begin{aligned} V_3^2 \notin A \triangleq &\{\frac{(\alpha_1\bar{h}_{11} + \alpha_2)V_1^1 + (\alpha_3\bar{h}_{11} + \frac{1}{\bar{h}}\alpha_4)V_1^2 + (\alpha_5\bar{h}_{11}\bar{h} + \alpha_6)V_2^1 + \alpha_7 V_2^2 + \alpha_8 V_3^1}{\beta_1\bar{h}_{11} + \beta_2} : \\ &\alpha_k \in \mathbb{F}_p, k \in \{1, \ldots, 8\}, (\beta_1, \beta_2) \neq (0, 0)\} \end{aligned} \tag{145}$$

$$\begin{aligned} V_3^2 \notin B \triangleq &\{\alpha_1 V_1^1 + (\alpha_2 + \alpha_3\frac{\bar{h}_{22}}{\bar{h}})V_1^2 + (\alpha_4\bar{h} + \alpha_5\bar{h}_{22})V_2^1 + (\alpha_6\bar{h}_{22} + \alpha_7)V_2^2 + (\alpha_8\bar{h}_{22} + \alpha_9)V_3^1 : \\ &\alpha_k, \beta_1, \beta_2 \in \mathbb{F}_p, k \in \{1, \ldots, 9\}\} \end{aligned} \tag{146}$$

$$\begin{aligned} V_3^2 \notin C \triangleq &\{\frac{(\alpha_1\bar{h}_{33} + \alpha_2)V_1^1 + \alpha_3 V_1^2 + \alpha_4\bar{h}V_2^1 + (\alpha_5\bar{h}_{33} + \alpha_6\bar{h})V_2^2 + (\alpha_7\bar{h}_{33} + \alpha_8\bar{h})V_3^1}{\beta_1\bar{h}_{33} + \beta_2} : \\ &\alpha_k, \beta_1, \beta_2 \in \mathbb{F}_p, k \in \{1, \ldots, 8\}, (\beta_1, \beta_2) \neq (0, 0)\} \end{aligned} \tag{147}$$

Now we note that

$$|A| \leq \frac{(p^2-1)p^8}{p-1} = p^9 + p^8, \qquad |B| \leq p^9, \qquad |C| \leq \frac{(p^2-1)p^8}{p-1} = p^9 + p^8 \tag{148}$$

$$|A \cup B \cup C| \leq 3p^9 + 2p^8 \tag{149}$$

There are p^{10} choices for V_3^2, and since

$$p^{10} \quad > \quad 3p^9 + 2p^8 \tag{150}$$

for $p > 3$, there exist choices for V_3^2 such that all 3 conditions (145),(146),(147) hold. Choosing V_3^2 from those, we note that all columns each of S_1, S_2, S_3 are linearly independent over $\mathbb{F}_p$.

Therefore, we have constructed beam forming vectors such that desired and interference signals are linearly independent at all destinations. This proves the achievability of linear-scheme capacity of $\frac{6}{5}$ for 3-user interference channel over $\mathbb{F}_{p^2}$ for all $p > 3$ when the specified conditions are met. For p=2 and p=3, we are able to exhaustively solve all possible cases numerically using MATLAB, completing the achievability proof of sum-rate $\frac{6}{5}$ for channel over $\mathbb{F}_{p^2}$ for all p under the conditions of Theorem 5.

The conditions can be also re-written in terms of the original channels as follows.

$$\begin{aligned}
\bar{h}_{11} = \frac{h_{11}h_{23}}{h_{13}h_{21}} \notin \mathbb{F}_p, \qquad & \bar{h}\bar{h}_{11} = \frac{h_{11}h_{32}}{h_{12}h_{31}} \notin \mathbb{F}_p \\
\bar{h}_{22} = \frac{h_{22}h_{13}}{h_{23}h_{12}} \notin \mathbb{F}_p, \qquad & \frac{\bar{h}}{\bar{h}_{22}} = \frac{h_{21}h_{32}}{h_{22}h_{31}} \notin \mathbb{F}_p \\
\bar{h}_{33} = \frac{h_{33}h_{21}}{h_{31}h_{23}} \notin \mathbb{F}_p, \qquad & \frac{\bar{h}}{\bar{h}_{33}} = \frac{h_{32}h_{13}}{h_{33}h_{12}} \notin \mathbb{F}_p
\end{aligned}$$

■

Remark 5: Note that these 6 conditions are equivalent to the 6 conditions on the phase differences between channel coefficients in the asymmetric complex signing scheme for wireless networks, as described in [7] to achieve DoF of $\frac{6}{5}$.

Remark 6: Each of the direct channels satisfy $\bar{h}_{ii} \notin \mathbb{F}_p, i \in \{1,2,3\}$ The fraction of channel realizations for which direct channels satisfy the 3 conditions is at least

$$(\frac{p^2-p}{p^2})^3 = (1-\frac{1}{p})^3 \rightarrow \ 1 \text{ for large } p \tag{151}$$

Further cross channel $\bar{h}$ should satisfy the conditions $\bar{h} \neq \frac{\alpha}{\bar{h}_{11}}, \bar{h} \neq \beta\bar{h}_{22}, \bar{h} \neq \gamma\bar{h}_{33}$ for $\alpha, \beta, \gamma \in \mathbb{F}_p$. There are atmost $3p$ channels such that one of these 3 conditions on $\bar{h}$ is violated. Hence there are at least $p^2 - 3p$ valid channel realizations for $\bar{h}$ for $p > 3$. Putting everything together, the fraction of all channels for which the scheme works for $p > 3$ is at least

$$(1-\frac{1}{p})^3(\frac{p^2-3p}{p^2}) = (1-\frac{1}{p})^3(1-\frac{3}{p}) \rightarrow \ 1 \text{ for large } p \tag{152}$$

3.6 Linear outer bound

In this section, we will prove the linear outer bounds. The proof follows along the lines of [29] by showing that the alignment depth can be at most D, which is a function of channel diversity (in case of finite fields, n).

3.6.1 Linear outer bound over $\mathbb{F}_{p^n}, n = 2l + 1$

Lemma 1 *Alignment depth is at most $D = 2n - \lfloor \frac{n}{2} \rfloor - 1$ for the normalized 3-user interference channel, wherein channels $\bar{h}, \bar{h}_{kk} \in \mathbb{F}_{p^n}$ for odd $n = 2l + 1$ and satisfy*

$$\bar{h}_{11} \notin A \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_{l-1}\bar{h}^{l-1}}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_l\bar{h}^l} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \right\} \quad (153)$$

$$\bar{h}_{22} \notin B \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_l\bar{h}^l}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_{l-1}\bar{h}^{l-1}} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_{l-1}) \neq (0, \ldots, 0) \right\} \quad (154)$$

$$\bar{h}_{33} \notin C \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_l\bar{h}^l}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_{l-1}\bar{h}^{l-1}} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_{l-1}) \neq (0, \ldots, 0) \right\} \quad (155)$$

$$\beta_l\bar{h}^l + \ldots + \beta_1\bar{h} + \beta_0 \neq 0 : \beta_0, \ldots, \beta_l \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \quad (156)$$

Proof: Let us consider the normalized channel as described in section 3.3 for odd $n = 2l + 1$, and at source 1, denote a vector of dimension $m \times 1$ as V with entries from $\mathbb{F}_{p^n}$. Since this is a converse proof, we assume that the desired symbols can be decoded at all the destinations. Here m denotes the number of symbol extensions of the channel. This vector of source 1 needs to be aligned with a vector from source 3 at destination 2, we can denote the vector at source 3 as $\gamma_1 V$ with $\gamma_1 \in \mathbb{F}_p$. Vector $\gamma_1 V$ aligns with a vector from source 2 at destination 1, say $\beta_1 V$ with $\beta_1 \in \mathbb{F}_p$. Vector $\beta_1 V$ aligns with a vector from source 1 at destination 3, say $\alpha_1\bar{h}V$ with $\alpha_1 \in \mathbb{F}_p$. So far, alignment chain length can be seen to be 4, and such an alignment chain can be extended upto length D when operating in field of order p^n. With $n = 2l + 1$ this results in source 1 using $l + 1$ vectors, and sources 2 and 3 using l vectors each such that the alignment chain length is $D = 3l + 1$. Then the vectors chosen so far at the 3 sources can be represented as

$$V_1 = [\alpha_l\bar{h}^l V \quad \alpha_{l-1}\bar{h}^{l-1}V \quad \ldots \quad \alpha_1\bar{h}V \quad V] \quad (157)$$

$$V_2 = [\beta_l\bar{h}^{l-1}V \quad \beta_{l-1}\bar{h}^{l-2}V \quad \ldots \quad \beta_2\bar{h}V \quad \beta_1 V] \quad (158)$$

$$V_3 = [\gamma_l\bar{h}^{l-1}V \quad \gamma_{l-1}\bar{h}^{l-2}V \quad \ldots \quad \gamma_2\bar{h}V \quad \gamma_1 V] \quad (159)$$

wherein V is an $m \times 1$ vector with entries from $\mathbb{F}_{p^n}$ and $\alpha_i, \beta_i, \gamma_i \in \mathbb{F}_p$, $\forall i \in \{1, \ldots, l\}$. We will now argue that alignment chain length cannot be extended beyond D. Suppose on the contrary, alignment chain length was greater than D, say $D + 1$. Then without loss of generality, we can choose additional vector at source 3 such that at destination 2, it aligns with the vector $\alpha_l\bar{h}^l V$ used at source 1. This additional vector at source 3 can be represented as $\gamma_{l+1}\bar{h}^l V$. Then the vectors sent by source 3 can be represented as

$$\bar{V}_3 = [\gamma_{l+1}\bar{h}^l V \quad \gamma_l\bar{h}^{l-1}V \quad \gamma_{l-1}\bar{h}^{l-2}V \quad \ldots \quad \gamma_2\bar{h}V \quad \gamma_1 V] \quad (160)$$

Let us consider the signal space at destination 1, $S_1 = [\bar{h}_{11}V_1 \;\; V_2 \;\; \bar{V}_3]$. Since l vectors from source 3 align with l vectors from source 2, we can denote the signal space as $S_1 = [\bar{h}_{11}V_1 \;\; V_2 \;\; \gamma_{l+1}\bar{h}^l V]$. Now we claim that $\bar{h}_{11}V_1$ and V_2 spans the channel space, since all vectors are linearly independent.

$$[\bar{h}_{11}V_1 \;\; V_2] = [\alpha_l\bar{h}_{11}\bar{h}^l V \;\; \alpha_{l-1}\bar{h}_{11}\bar{h}^{l-1}V \;\; \ldots \;\; \alpha_1\bar{h}_{11}\bar{h}V \;\; \bar{h}_{11}V \;\; \beta_l\bar{h}^{l-1}V \;\; \beta_{l-1}\bar{h}^{l-2}V \;\; \ldots \;\; \beta_2\bar{h}V \;\; \beta_1 V]$$

It can be noted that columns of above matrix are linearly independent when all entries listed below are linearly independent, since V is scaled by different powers of $\bar{h}, \bar{h}_{11}$ and other coefficients.

$$[\alpha_l \bar{h}_{11}\bar{h}^l \;\; \alpha_{l-1}\bar{h}_{11}\bar{h}^{l-1} \;\; \ldots \;\; \alpha_1\bar{h}_{11}\bar{h} \;\; \bar{h}_{11} \;\; \beta_l\bar{h}^{l-1} \;\; \beta_{l-1}\bar{h}^{l-2} \;\; \ldots \;\; \beta_2\bar{h} \;\; \beta_1]$$

This is true when following conditions on $\bar{h}, \bar{h}_{11}$ are met.

$$\bar{h}_{11} \notin A \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_{l-1}\bar{h}^{l-1}}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_l\bar{h}^l} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \right\} \quad (161)$$

$$\beta_l\bar{h}^l + \ldots + \beta_1\bar{h} + \beta_0 \neq 0 : \beta_0, \ldots, \beta_l \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \quad (162)$$

Since $n = 2l + 1$ columns of $[\bar{h}_{11}V_1 \;\; V_2]$ are linearly independent, additional vector chosen $\gamma_{l+1}\bar{h}^l V$ must lie in span of $[\bar{h}_{11}V_1 \;\; V_2]$. It cannot lie in the space spanned by V_2 because that would contradict (156). But if it does not lie in the space spanned by V_2 then the desired signal space $\bar{h}_{11}V_1$ cannot be resolvable from interference. This is a contradiction, since in the converse we assume that the desired signal is resolvable from interference. Therefore additional vector $\gamma_{l+1}\bar{h}^l V$ cannot be chosen at source 3 such that it aligns at destination 1, i.e., alignment depth cannot be greater than $D = 3l + 1$. This is illustrated in Fig. 13. Similarly alignment chains originating at other sources and ending at other destinations can be shown to be of depth not greater than D. Consolidating the linear independence conditions for all such chains, we note that alignment depth is at most D for channels satisfying following conditions.

$$\bar{h}_{11} \notin A \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_{l-1}\bar{h}^{l-1}}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_l\bar{h}^l} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \right\} \quad (163)$$

$$\bar{h}_{22} \notin B \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_l\bar{h}^l}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_{l-1}\bar{h}^{l-1}} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_{l-1}) \neq (0, \ldots, 0) \right\} \quad (164)$$

$$\bar{h}_{33} \notin C \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_l\bar{h}^l}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_{l-1}\bar{h}^{l-1}} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_{l-1}) \neq (0, \ldots, 0) \right\} \quad (165)$$

$$\beta_l\bar{h}^l + \ldots + \beta_1\bar{h} + \beta_0 \neq 0 : \beta_0, \ldots, \beta_l \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \quad (166)$$

Thus, we have proved Lemma 1.

We now show the outer bound on linear-scheme capacity for 3-user interference channel to be $\frac{3D}{2D+1}$. The proof of this part is almost identical to that in [29], so it is summarized only for the sake of completeness.

Theorem 6 *For the 3-user interference channel over $\mathbb{F}_{p^n}$, outer bound on linear-scheme capacity is given by $\frac{3D}{2D+1}$, with $D = 2n - \lfloor \frac{n}{2} \rfloor - 1$ for odd $n = 2l + 1$ wherein channels satisfy the following conditions*

$$\bar{h}_{11} \notin A \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_{l-1}\bar{h}^{l-1}}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_l\bar{h}^l} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \right\} \quad (167)$$

$$\bar{h}_{22} \notin B \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_l\bar{h}^l}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_{l-1}\bar{h}^{l-1}} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_{l-1}) \neq (0, \ldots, 0) \right\} \quad (168)$$

$$\bar{h}_{33} \notin C \triangleq \left\{ \frac{\alpha_0 + \alpha_1\bar{h} + \ldots + \alpha_l\bar{h}^l}{\beta_0 + \beta_1\bar{h} + \ldots + \beta_{l-1}\bar{h}^{l-1}} : \alpha_k, \beta_m \in \mathbb{F}_p, (\beta_0, \ldots, \beta_{l-1}) \neq (0, \ldots, 0) \right\} \quad (169)$$

$$\beta_l\bar{h}^l + \ldots + \beta_1\bar{h} + \beta_0 \neq 0 : \beta_0, \ldots, \beta_l \in \mathbb{F}_p, (\beta_0, \ldots, \beta_l) \neq (0, \ldots, 0) \quad (170)$$

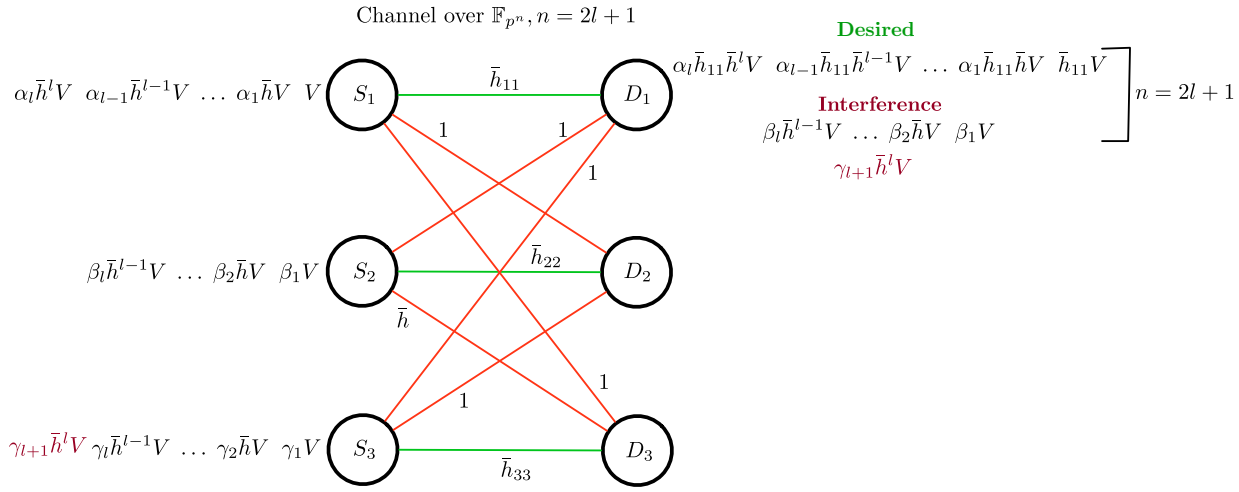

Figure 13: Alignment depth in 3-user Interference channel

Proof: Let $V_{i\uparrow k}$ denote the signal space of user i (part of V_i) aligned to depth $k+1$ and $d_i = \dim(V_i), d_{i\uparrow k} = \dim(V_{i\uparrow k})$. Lemma 8 of [29] follows since we have finite dimensional subspaces, i.e., $d_{i\uparrow k} \geq d_{i\uparrow k+a} + d_{i-b\uparrow k+b} - d_{i-b\uparrow k+a+b}$. For $a=-1, b=-1$, we have

$$d_{i\uparrow k} \geq d_{i\uparrow k-1} + d_{i+1\uparrow k-1} - d_{i+1\uparrow k-2} \tag{171}$$

Since alignment depth is at most D (Lemma 1), $V_{i\uparrow D} = \{0\}$ for each i, and so similar to lemma 9 of [29], we have

$$d_i \geq d_{i-1\uparrow 1} + d_{i\uparrow D-1} \tag{172}$$

Let us denote $c_k = \sum_{i=1}^{3} d_{i\uparrow k}$. Then using 171, we have $c_k \geq 2c_{k-1} - c_{k-2}$. Using induction, it can be deduced that $c_k \geq ic_{k-i+1} - (i-1)c_{k-i}$. For $i = k = D-1$, we have

$$(D-2)c_0 \geq (D-1)c_1 - c_{D-1} \tag{173}$$

Using 172, it can be shown that $c_0 \geq c_1 + c_{D-1}$. Combining with 173, we have $(D-1)c_0 \geq Dc_1$. Let total dimension at each destination be denoted by $N = mn$ where m symbol extensions of the channel is considered with channels from $\mathbb{F}_{p^n}$. Since interference span must be linearly independent of desired signal, and considering N dimensions at destination 1, we have

$$\text{Destination 1:} \quad \dim(\bar{h}_{11}V_1 + V_2 + V_3) = \quad d_1 + d_2 + d_3 - d_{2\uparrow 1} \leq N \tag{174}$$

$$\text{Destination 2:} \quad \dim(V_1 + \bar{h}_{22}V_2 + V_3) = \quad d_1 + d_2 + d_3 - d_{3\uparrow 1} \leq N \tag{175}$$

$$\text{Destination 3:} \quad \dim(V_1 + \bar{h}V_2 + \bar{h}_{33}V_3) = \quad d_1 + d_2 + d_3 - d_{1\uparrow 1} \leq N \tag{176}$$

Adding above inequalities and using $(D-1)c_0 \geq Dc_1$, we can deduce as in [29] that

$$\frac{d_1 + d_2 + d_3}{N} \leq \frac{3D}{2D+1} \tag{177}$$

Thus we have proved the outer bound on linear-scheme capacity for 3-user interference channel over $\mathbb{F}_{p^n}$ with channels satisfying aforementioned linear independence constraints. ■

4 Conclusion

Linear capacity results are explored for the X channel and the 3 user interference channel over the finite field $\mathbb{F}_{p^n}$, by translating precoding based interference alignment schemes from corresponding DoF results for the wireless setting. The main insight is that the finite field $\mathbb{F}_{p^n}$ can be viewed as analogous to diagonal $n \times n$ wireless channels with diversity n. This insight appears to be broadly true for linear precoding based schemes. While the linear capacity is fully characterized, the information theoretic capacity remains open for finite field networks over $\mathbb{F}_p$, i.e., for $n = 1$, where diversity is only 1. We expect that signal level alignment schemes and combinatorial outer bound arguments such as those presented in [32] should be useful in these cases.

5 Appendix

5.1 Appendix I - X channel over $\mathbb{F}_{p^3}$: Alternate proof

Here we discuss an alternate proof for achievability of sum rate of $\frac{4}{3}$ for 2-user X channel over $\mathbb{F}_{p^3}$. Let us first state a lemma.

Definition 1: Let $\mathbb{F}_{p^n}$ be the field extension of $\mathbb{F}_p$, and $p(x)$ the ring of polynomials in x over $\mathbb{F}_p$. The minimal polynomial of $h \in \mathbb{F}_{p^n}$ is the monic polynomial of least degree among all polynomials such that $p(h) = 0$.

Lemma 2 *For $h \in \mathbb{F}_{p^n}$ with both p, n being prime, $1, h, h^2, \ldots, h^{n-1}$ are linearly independent over $\mathbb{F}_p$ if and only if $h \notin \mathbb{F}_p$*

$$\alpha_0 + \alpha_1 h + \alpha_2 h^2 + \cdots + \alpha_{n-1} h^{n-1} \neq 0 \iff h \notin \mathbb{F}_p \tag{178}$$

wherein $\alpha_k \in \mathbb{F}_p, k \in \{0, 1, \ldots, n-1\}$.

Proof: When $1, h, h^2, \ldots, h^{n-1}$ are linearly independent over $\mathbb{F}_p$, it is trivial to note that $h \notin \mathbb{F}_p$. For the other direction, let us consider $h \notin \mathbb{F}_p$. Suppose on the contrary, $1, h, h^2, \ldots, h^{n-1}$ were linearly dependent over $\mathbb{F}_p$, then there exist $\alpha_k \in \mathbb{F}_p, k \in \{0, 1, \ldots, n-1\}$ such that

$$\alpha_0 + \alpha_1 h + \alpha_2 h^2 + \cdots + \alpha_{n-1} h^{n-1} = 0 \tag{179}$$

If (179) holds, one can identify a monic irreducible polynomial of degree $k \leq n-1$, which is then the minimal polynomial of $h \in \mathbb{F}_{p^n}$ according to definition 1. From Theorem 3.33 of [36], we note that degree of minimal polynomial of an element $h \in \mathbb{F}_{p^n}$ (in our case, degree is k), divides n. As a result, since we consider only prime n, $k > 1$ is not possible. k cannot be 1 since $h \notin \mathbb{F}_p$. Hence (179) is a contradiction, and so $1, h, h^2, \ldots, h^{n-1}$ are linearly independent over $\mathbb{F}_p$ when $h \notin \mathbb{F}_p$. ■

Achievability for Theorem 2 over $\mathbb{F}_{p^3}$:
For the fully connected X channel over $\mathbb{F}_{p^3}$ if $h = \frac{h_{12}h_{21}}{h_{11}h_{22}} \notin \mathbb{F}_p$, then $C = C_{\text{linear}} = \frac{4}{3}$. in units of $\mathbb{F}_{p^3}$ symbols per channel use.

Alternate *Proof:* Like in section 2.6, for the 2-user X channel, the received symbols after precoding using beamforming vectors $v_{ji} \in \mathbb{F}_{p^3}$ for input symbols $x_{ji} \in \mathbb{F}_p$, are expressed as

$$\begin{aligned} y_1 &= v_{11}x_{11} + v_{12}x_{12} + v_{22}x_{22} + v_{21}x_{21} \\ y_2 &= v_{22}x_{22} + hv_{21}x_{21} + hv_{11}x_{11} + v_{12}x_{12} \end{aligned}$$

wherein $h, y_j \in \mathbb{F}_{p^3}$. Interference is aligned at each destination along one dimension by setting $v_{22} = v_{21}$ and $v_{12} = hv_{11}$. At the destinations, signal spaces are represented using matrices S_1 and S_2.

$$S_1 = [v_{11} \quad v_{12} \quad v_{21}] = [v_{11} \quad hv_{11} \quad v_{21}] \tag{180}$$

$$S_2 = [v_{22} \quad hv_{21} \quad v_{12}] = [v_{21} \quad hv_{21} \quad hv_{11}] \tag{181}$$

Let us choose $v_{21} = 1, v_{11} = h$. Then S_1, S_2 are identical, given by

$$S_1 = S_2 = [1 \quad h \quad h^2] \tag{182}$$

Using Lemma 2, it follows that for all $h \in \mathbb{F}_{p^3}$, field elements $1, h, h^2$ are linearly independent over $\mathbb{F}_p$ if $h \notin \mathbb{F}_p$. Hence, desired and interfering symbols are linearly independent over $\mathbb{F}_p$ when $h \notin \mathbb{F}_p$.

Thus, we have proved the achievability of rate $\frac{1}{3}$ per message, and a sum-rate of $\frac{4}{3}$, which matches the capacity outer bound. ■

5.2 Appendix II - X Channel over $\mathbb{F}_{p^2}$

$\mathbb{F}_{p^2}$ can be viewed as a 2-dimensional vector space over subfield $\mathbb{F}_p$, much like the field of complex numbers can be viewed as a 2-dimensional vector space over reals ($\mathbb{R}$), which is also the essential idea behind the asymmetric complex signaling scheme used in [7] to achieve 4/3 DoF for the constant SISO wireless X channel with complex coefficients. We can represent each element of $\mathbb{F}_{p^2}$ as

$$z = x + y\sqrt{c} \quad \text{or} \quad x + ys \tag{183}$$

wherein $z \in \mathbb{F}_{p^2}$, $x, y \in \mathbb{F}_p$ and c is a quadratic non-residue (an element that does not have a square root in $\mathbb{F}_p$) similar to -1 (which does not have a square root over reals) in the field of complex numbers. ($s = \sqrt{c} \equiv j$).

For example, consider $\mathbb{F}_{3^2}$ with prime subfield $\mathbb{F}_3$ which has $c = -1 (\text{mod } 3) = 2$ as the quadratic non-residue, since $\sqrt{2}$ does not exist in $\mathbb{F}_3$. Field $\mathbb{F}_{3^2}$ contains 9 elements and every element $a_1 s + a_0$ can be written in a vector notation with coefficients $[a_1; a_0]$ wherein $a_1, a_0 \in \mathbb{F}_3 = \{0, 1, 2\}$ and assigned a scalar integer label $\{0, 1, \ldots, 8\}$ as $3a_1 + a_o$. For example, the field element labeled $a = 7$ can be represented as $[2\ ;\ 1]$ in vector notation, as $2s + 1$ in polynomial notation, or as $2\sqrt{2} + 1$ in the quadratic non-residue notation.

Here, product with h can be represented using a 2×2 linear transformation (MIMO equivalent). Let $h = h_1 s + h_0, \quad x = x_1 s + x_0$ and $h_i, x_i \in \mathbb{F}_3$. Then the product $y = hx \in \mathbb{F}_{3^2}$ can be written as

$$y = hx = (h_1 s + h_0)(x_1 s + x_0) = s^2(h_1 x_1) + s(h_1 x_0 + h_0 x_1) + (h_0 x_0) \tag{184}$$

and in vector notation as

$$\mathbf{y} = \mathbf{H}\mathbf{x} = \begin{bmatrix} h_0 & 2h_1 \\ h_1 & h_0 \end{bmatrix} \begin{bmatrix} x_1 \\ x_0 \end{bmatrix} \tag{185}$$

wherein $\mathbf{x} \in \mathbb{F}_3^{2\times 1}$ and $\mathbf{H} \in \mathbb{F}_3^{2\times 2}$. It can be noted that above 2×2 linear transformation is equivalent to complex multiplication and stacking the resulting real and imaginary parts in a 2×1 vector. Note that $\mathbb{F}_2$ is a special case because there is no quadratic non-residue, where the scheme is equivalent to having a 2×2 MIMO channel, but not to asymmetric complex signaling.

Achievability proof for X-channel over $\mathbb{F}_{p^2}$

Proof: Now we prove that sum rate of $\frac{4}{3}$ is achievable (part of Theorem 2 proof) for 2-user X-channel over $\mathbb{F}_{p^2}$. We consider the X channel with 3 symbol extensions, wherein we can represent the channel between source i and destination j as $H_{ji} = h_{ji}I_3$ where I_3 is the 3×3 identity matrix and h_{ji} is the scalar channel coefficient from $\mathbb{F}_{p^2}$. The inputs x_{ji} are chosen from $\mathbb{F}_p$ and outputs y_j over $\mathbb{F}_{p^2}$ and three channel uses can be seen as a 6 dimensional vector space over $\mathbb{F}_p$ within which 4 desired symbols and 4 interference symbols are present at each destination. In order to achieve capacity, interference should be aligned within 2 dimensions at each destination. To this end, we will construct beamforming vectors at each source such that interference is aligned. Received symbols at the destinations, in vector notation, are given by

$$\begin{aligned}\mathbf{Y}_1 &= \mathbf{V}_{11}X_{11} + \mathbf{V}_{12}X_{12} + \mathbf{V}_{22}X_{22} + \mathbf{V}_{21}X_{21} \\ \mathbf{Y}_2 &= \mathbf{V}_{22}X_{22} + \bar{\mathbf{H}}\mathbf{V}_{21}X_{21} + \bar{\mathbf{H}}\mathbf{V}_{11}X_{11} + \mathbf{V}_{12}X_{12}\end{aligned}$$

Here $\mathbf{Y}_j \in \mathbb{F}_p^{6\times 1}, \mathbf{V}_{ji} \in \mathbb{F}_p^{6\times 2}$, and $X_{ji} \in \mathbb{F}_p^{2\times 1}$ represents the symbols sent by source i for destination j. $\bar{\mathbf{H}} \in \mathbb{F}_p^{6\times 6}$ is the linear transformation which is equivalent to multiplication by $h \in \mathbb{F}_{p^2}$. Over 3 symbol extensions of the channel, linear transformation $\bar{\mathbf{H}}$ for $p > 2$, is given by

$$\bar{\mathbf{H}} = \begin{bmatrix} h_0 & 0 & 0 & ch_1 & 0 & 0 \\ 0 & h_0 & 0 & 0 & ch_1 & 0 \\ 0 & 0 & h_0 & 0 & 0 & ch_1 \\ h_1 & 0 & 0 & h_0 & 0 & 0 \\ 0 & h_1 & 0 & 0 & h_0 & 0 \\ 0 & 0 & h_1 & 0 & 0 & h_0 \end{bmatrix} \tag{186}$$

Note that above matrix is the 3-symbol extension of the linear transformation $H = [h_0 \;\; ch_1; h_1 \;\; h_0]$. Here, c is the quadratic non-residue which exists for all $p > 2$. In order to achieve sum rate of $\frac{4}{3}$, interference should be aligned at both destinations:

$$\text{span}(\mathbf{V}_{22}) \equiv \text{span}(\mathbf{V}_{21}) \quad \& \quad \text{span}(\mathbf{V}_{12}) \equiv \text{span}(\bar{\mathbf{H}}\mathbf{V}_{11}) \tag{187}$$

For every choice of $\mathbf{V}_{21}, \mathbf{V}_{11}$, we set

$$\mathbf{V}_{22} = \mathbf{V}_{21} \qquad \& \qquad \mathbf{V}_{12} = \bar{\mathbf{H}}\mathbf{V}_{11} \tag{188}$$

At each destination, the two desired signal vectors and the aligned interference vector can be represented using 6×6 matrices, S_1 and S_2.

$$S_1 = [\mathbf{V}_{11} \;\; \mathbf{V}_{12} \;\; \mathbf{V}_{21}] = [\mathbf{V}_{11} \;\; \bar{\mathbf{H}}\mathbf{V}_{11} \;\; \mathbf{V}_{21}] \tag{189}$$

$$S_2 = [\mathbf{V}_{22} \;\; \bar{\mathbf{H}}\mathbf{V}_{21} \;\; \mathbf{V}_{12}] = [\mathbf{V}_{21} \;\; \bar{\mathbf{H}}\mathbf{V}_{21} \;\; \bar{\mathbf{H}}\mathbf{V}_{11}] \tag{190}$$

We now choose $\mathbf{V}_{11}$ and $\mathbf{V}_{21}$ as follows.

$$\mathbf{V}_{11} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \\ 0 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \end{bmatrix} \qquad\qquad \mathbf{V}_{21} = \begin{bmatrix} 1 & 0 \\ 1 & 0 \\ 1 & 1 \\ 0 & 0 \\ 1 & 1 \\ 1 & 1 \end{bmatrix} \tag{191}$$

With above choice of beamforming matrices, matrices S_1 and S_2 can be written as

$$S_1 = \begin{bmatrix} 1 & 1 & h_0+ch_1 & h_0+ch_1 & 1 & 0 \\ 1 & 0 & h_0 & ch_1 & 1 & 0 \\ 0 & 0 & 0 & ch_1 & 1 & 1 \\ 1 & 1 & h_0+h_1 & h_0+h_1 & 0 & 0 \\ 0 & 1 & h_1 & h_0 & 1 & 1 \\ 0 & 1 & 0 & h_0 & 1 & 1 \end{bmatrix} \quad S_2 = \begin{bmatrix} h_0 & 0 & h_0+ch_1 & h_0+ch_1 & 1 & 0 \\ h_0+ch_1 & ch_1 & h_0 & ch_1 & 1 & 0 \\ h_0+ch_1 & h_0+ch_1 & 0 & ch_1 & 1 & 1 \\ h_1 & 0 & h_0+h_1 & h_0+h_1 & 0 & 0 \\ h_0+h_1 & h_0 & h_1 & h_0 & 1 & 1 \\ h_0+h_1 & h_0+h_1 & 0 & h_0 & 1 & 1 \end{bmatrix}$$

Evaluating determinant of the above two matrices, we get the following polynomials

$$|S_1| = ch_1^2 \tag{192}$$

$$|S_2| = h_1^2(ch_1^2 - h_0^2) \tag{193}$$

Determinant of matrix S_1 is non-zero since $h_1 \neq 0$ when $h \notin \mathbb{F}_p$, and a non-zero quadratic non-residue exists for all $p > 2$, i.e., $c \neq 0$. When considering determinant polynomial of matrix S_2, term $h_1^2 \neq 0$ when $h \notin \mathbb{F}_p$. Therefore, $|S_2| = 0$ only when $c = \frac{h_0^2}{h_1^2}$. But this is clearly not possible since the quadratic non-residue, c cannot be a square of any element in $\mathbb{F}_p$ ($\frac{h_0}{h_1} \in \mathbb{F}_p$). Hence, columns of matrices S_1 and S_2 are linearly independent over $\mathbb{F}_p$, implying that the desired and interference signals do not overlap.

For the case of p=2, we are able to solve all possible cases numerically using MATLAB by constructing beamforming matrices $\mathbf{V}_{11}$ and $\mathbf{V}_{21}$ such that the columns of matrices S_1 and S_2 are linearly independent. Thus, when $h \notin \mathbb{F}_p$, we have shown that the desired signals are resolvable, and sum rate of $\frac{4}{3}$ is achievable for channels over $\mathbb{F}_{p^2}$ for all p.

5.3 Appendix III - Zero Channels in 3-user Interference channel

Here, we deal with realizations of the 3-user interference channel where some of the channel coefficients are zero.

Theorem 7 *For the 3 user interference channel over $\mathbb{F}_{p^n}$, if one or more of the channel coefficients h_{ji} is equal to zero, the capacity results are given as follows:*

1. *If all three direct channels are zero, then $C = C_{linear} = 0$.*
2. *If any two direct channels are zero, then $C = C_{linear} = 1$.*
3. *If exactly one direct channel is zero, then $C = C_{linear} = 1$ or $C = C_{linear} = 2$, depending on whether any of the cross-channels between the other two users takes a non-zero value or they are all zero, respectively.*
4. *If all direct channels are non-zero and all 6 cross channels are zero, then $C = C_{linear} = 3$.*
5. *If all direct channels are non-zero and either 4 or 5 cross channels are zero, then $C = C_{linear} = 2$.*
6. *If all direct channels are non-zero and either 2 or 3 cross channels are zero, and if $h_{ij} = h_{ji} = 0$ for any one $\{i, j\} \in \{1, 2, 3\}$, then $C = C_{linear} = 2$.*

7. *In all other cases, the linear capacity is either* 1 *or* 1.5 *for channels over* $\mathbb{F}_{p^n}$ *with* $p > 3$ *(the specific cases for each are identified in the proof).*

Proof: Cases 1,2,3,4,6 are trivial. The remaining cases are discussed below.
Case 5: For all these channel structures, it can be shown that there always exists at least one $\{i, j\} \in \{1, 2, 3\}$ such that $h_{ij} = h_{ji} = 0$, and so only the sources $\{i, j\}$ can be used for transmission, leading to a sum rate of 2 being achievable. Outer bound of 2 follows by removing all but one non-zero cross-link.

Case 7:
For the achievability of sum rate of 1.5, consider the following:

1. All channels are from $\mathbb{F}_{p^n}$. For even $n = 2l$, we choose beamforming matrices $V \in \mathbb{F}_{p^n}^{1\times l}$ at some of the sources and $V' \in \mathbb{F}_{p^n}^{1\times l}$ at others, and precode $\frac{n}{2} = l$ symbols $x_k^1, x_k^2, \ldots, x_k^l \in \mathbb{F}_p$ for each channel use, at all 3 sources. We denote the l columns of V as $v_1, v_2, \ldots, v_l$ and those of V' as $v_1', v_2', \ldots, v_l'$. These beam forming matrices would be chosen such that desired and interference symbols are linearly independent over $\mathbb{F}_p$ at the destinations.

2. When n is odd, 2 symbol extensions are used wherein the beamforming matrix $V \in \mathbb{F}_{p^n}^{2\times n}$ is used at some of the sources and $V' \in \mathbb{F}_{p^n}^{2\times n}$ at others. Over 2 channel uses, n input symbols are precoded at each source. Columns of V and V' are then chosen such that desired and interference symbols are linearly independent over $\mathbb{F}_p$ at all destinations. Linear independence arguments follow similar to case of even n.

We describe only even n for various channel structures, for brevity.

Let us first consider the setting where 3 cross channels are zero. There are 5 distinct channel structures corresponding to any three cross channels being zero, and all other channel structures ($\binom{6}{3} - 5 = 15$) are isomorphic to them. These 5 channel structures are shown in Fig. 14. Of these, A, B, C belong to Case 5, and are therefore trivial.

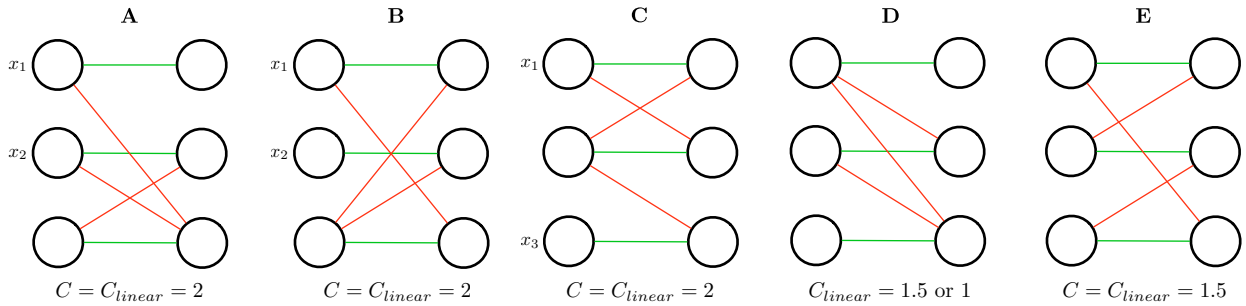

Figure 14: Distinct channel structures with 3 cross channels as 0

Structure D:
For this structure, interference from sources 1 and 2 need to be aligned at destination 3. The normalized channel for this structure is illustrated in Fig. 15.
Beam forming matrix V is used at sources 1 and 2, and V' is used at source 3. Signal spaces at 3

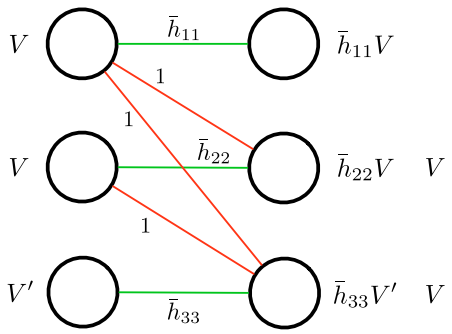

Figure 15: Normalized channel of structure D

destinations are then given by

$$S_1 = [\bar{h}_{11}V] = [\bar{h}_{11}v_1, \quad \bar{h}_{11}v_2, \quad \ldots, \quad \bar{h}_{11}v_l] \tag{194}$$

$$S_2 = [\bar{h}_{22}V \quad V] = [\bar{h}_{22}v_1, \quad \bar{h}_{22}v_2, \quad \ldots, \quad \bar{h}_{22}v_l, \quad v_1, \quad v_2, \quad \ldots, \quad v_l] \tag{195}$$

$$S_3 = [\bar{h}_{33}V' \quad V] = [\bar{h}_{33}v'_1, \quad \bar{h}_{33}v'_2, \quad \ldots, \quad \bar{h}_{33}v'_l \quad v_1, \quad v_2, \quad \ldots, \quad v_l] \tag{196}$$

Consider signal space at destination 2. Let us choose v_1 as 1, then if $\bar{h}_{22} \notin \mathbb{F}_p$, $[\bar{h}_{22}v_1 \quad v_1]$ are linearly independent over $\mathbb{F}_p$. Now let us construct v_2 such that 4 columns of S_2, $[\bar{h}_{22}v_1 \quad v_1 \quad \bar{h}_{22}v_2 \quad v_2]$ are linearly independent over $\mathbb{F}_p$.

$$\text{From } S_2, \quad v_2 \notin A \quad \triangleq \quad \left\{ \frac{(\alpha_1\bar{h}_{22} + \alpha_2)v_1}{\beta_1\bar{h}_{22} + \beta_2} : \alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}_p, (\beta_1, \beta_2) \neq (0,0) \right\} \tag{197}$$

Now we note that

$$|A| \quad \leq \quad \frac{(p^2-1)p^2}{p-1} = p^3 + p^2 \tag{198}$$

There are p^n choices for v_2, and since $p^n > (p^3 + p^2)$ for all p, there exist choices for v_2 such that condition (197) holds. Choosing v_2 from those, we note that 4 columns of S_2 are linearly independent over $\mathbb{F}_p$. We proceed recursively in a similar manner, for choosing columns $v_3, v_4, \ldots, v_{l-1}$ such that $6, 8, \ldots, 2(l-1)$ columns are linearly independent over $\mathbb{F}_p$ respectively, in S_2.

Let us now discuss the last iteration wherein we choose column v_l such that all $n = 2l$ columns are linearly independent over $\mathbb{F}_p$ in S_2, given that $2l-2$ columns are already linearly independent with appropriate choices of $v_1, v_2, \ldots, v_{l-1}$.

$$\text{From } S_2, \quad v_l \notin A \triangleq \{ \frac{(\alpha_1\bar{h}_{22} + \alpha_2)v_1 + (\alpha_3\bar{h}_{22} + \alpha_4)v_2 + \cdots + (\alpha_{2l-3}\bar{h}_{22} + \alpha_{2l-2})v_{l-1}}{\beta_1\bar{h}_{22} + \beta_2} : \\ \alpha_i, \beta_1, \beta_2 \in \mathbb{F}_p, i \in \{1, \ldots, 2l-2\}, (\beta_1, \beta_2) \neq (0,0)\} \tag{199}$$

Now we note that

$$|A| \quad \leq \quad \frac{(p^2-1)p^{2l-2}}{p-1} = p^{2l-1} + p^{2l-2} \tag{200}$$

There are $p^n = p^{2l}$ choices for v_l, and since $p^{2l} > (p^{2l-1} + p^{2l-2})$ for all p, there exist choices for v_l such that condition (199) holds. Choosing v_l from those, we note that all n columns of S_2 are linearly independent over $\mathbb{F}_p$. Also, it can be noted that $l = \frac{n}{2}$ columns of V in S_1 and S_3 are linearly independent over $\mathbb{F}_p$. Destination 1 does not receive any interference and so desired symbols are resolvable.

Let us now consider destination 3 where interference is aligned in $\frac{n}{2} = l$ linearly independent columns of V. Since source 3 does not cause interference anywhere, V' is trivially chosen to be $\frac{1}{\bar{h}_{33}}$ times the remaining $n/2$ basis vectors. Hence, desired and interference symbols are linearly independent at all destinations. Thus, sum rate of $\frac{3}{2}$ is achieved for structure D in Fig. 15, with channels over $\mathbb{F}_{p^n}$ for all even n, if $\bar{h}_{22} \notin \mathbb{F}_p$.

Fraction of channels for which scheme achieves $\frac{3}{2}$ sum rate is given by

$$\frac{p^n - p}{p^n} = 1 - \frac{1}{p^{n-1}} \to 1 \text{ for large } p, n \tag{201}$$

$\frac{3}{2}$ is also an information theoretic outer bound on sum rate for structure D because the sum-rate of any two users is bounded by 1. However, when $\bar{h}_{22} = 1$, then arguing along the lines of [31] we find that destination 3 can decode all three messages, so that the information theoretic sum-capacity bound = 1. For all other cases where $\bar{h}_{22} \in \mathbb{F}_p$ but $\bar{h}_{22} \notin \{0, 1\}$, the linear capacity is still 1 (because the linear capacity does not depend on the scaling of channel coefficients by non-zero $\mathbb{F}_p$ elements) but the information theoretic capacity is unknown.

Thus, structure D has linear capacity of 1.5 if $\bar{h}_{22} \notin \mathbb{F}_p$, and 1 otherwise.

Structure E: For structure E, the sum rate of 1.5 is achieved even without channel knowledge at the transmitters. For example, transmitter 1 sends an $\mathbb{F}_{p^n}$ symbol only over the first channel use and stays quiet over the second channel use, transmitter 2 sends a $\mathbb{F}_{p^n}$ symbol over the second channel use and remains quiet over the first channel use, and transmitter 3 repeats its $\mathbb{F}_{p^n}$ symbol over both channel uses. This allows each receiver to decode its desired symbols. The outer bound of 1.5 applies because the sum-capacity of any two users is 1. Thus, structure E has $C = C_{linear} = 1.5$.

Next let us consider cases where 2 cross channels are 0, shown in Fig. 16. Structure F belongs to Case 5, so it is trivial.

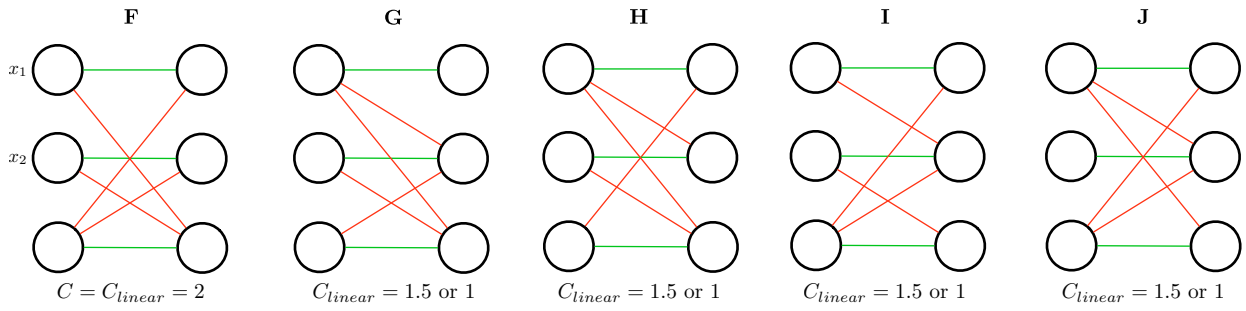

Figure 16: Distinct channel structures with 2 cross channels as 0

Structure G: The normalized channel for this structure is illustrated in Fig. 17. For this structure, signals from sources 1 and 2 need to be aligned at destination 3 and remain resolvable at destination 2. Following the proof for structure D, this can be done if $\bar{h}_{22} \notin \mathbb{F}_p$. Similarly, signals from sources 1 and 3 need to align at destination 2 and remain resolvable at destination 3. This can be done if $\bar{h}_{33} \notin \mathbb{F}_p$. We choose V such that both $S_2 = [\bar{h}_{22}V \quad V]$ and $S_3 = [\bar{h}_{33}V \quad V]$ are linearly independent over $\mathbb{F}_p$, which can be shown to be possible for all $p > 2$. Thus, sum rate of $\frac{3}{2}$ is achieved for structure G in Fig. 17, with channels over $\mathbb{F}_{p^n}$ for all even n, if $\bar{h}_{22}, \bar{h}_{33} \notin \mathbb{F}_p$. The outer bound of $\frac{3}{2}$ follows from the pair-wise bounds. If all non-zero channels are equal to 1, then the argument of [31] shows that one destination can decode all messages, i.e., $C = C_{linear} = 1$. In all other cases with non-zero $\bar{h}_{kk} \in \mathbb{F}_p$ for any $k = 2, 3$, the linear capacity is still one because the linear capacity is not affected by a scaling of channel coefficients by non-zero constants in $\mathbb{F}_p$. Thus structure G has linear-scheme capacity of $\frac{3}{2}$ if $\bar{h}_{kk} \notin \mathbb{F}_p, k \in \{2, 3\}$, and 1 otherwise.

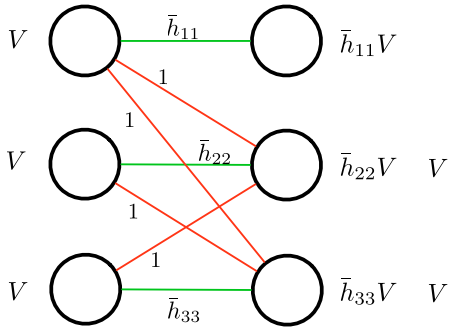

Figure 17: Normalized channel - structure G

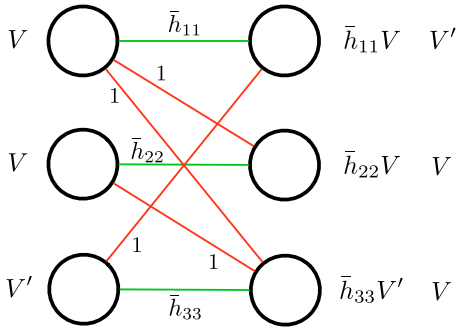

Figure 18: Normalized channel - structure H

Structure H:
The normalized channel for this structure is illustrated in Fig. 18. For this structure, signals from sources 1 and 2 need to be aligned at destination 3 and remain resolvable at destination 2. Following the proof for structure D, this can be done if $\bar{h}_{22} \notin \mathbb{F}_p$. We choose V' such that both $S_1 = [\bar{h}_{11}V \quad V']$ and $S_3 = [\bar{h}_{33}V' \quad V]$ are linearly independent over $\mathbb{F}_p$, which can be shown to be possible for all $p > 2$. Thus, sum rate of $\frac{3}{2}$ is achieved for structure H in Fig. 18, with channels over $\mathbb{F}_{p^n}$ for all even n, if $\bar{h}_{22} \notin \mathbb{F}_p$. The outer bound of $\frac{3}{2}$ follows from the pair-wise bounds. If all non-zero channels are equal to 1, then the argument of [31] shows that one destination can decode all messages, i.e., $C = C_{linear} = 1$. In all other cases with non-zero $\bar{h}_{22} \in \mathbb{F}_p$, the linear capacity is still one because the linear capacity is not affected by a scaling of channel coefficients by non-zero constants in $\mathbb{F}_p$. Thus structure H has linear-scheme capacity of $\frac{3}{2}$ if $\bar{h}_{22} \notin \mathbb{F}_p$, and 1 otherwise.

Structure I:
The normalized channel for this structure is illustrated in Fig. 19. For this structure, signals from sources 1 and 3 need to be aligned at destination 2 and remain resolvable at destination 1. Following the proof for structure D, this can be done if $\bar{h}_{11} \notin \mathbb{F}_p$. We choose V' such that both $S_2 = [\bar{h}_{22}V' \quad V]$ and $S_3 = [\bar{h}_{33}V \quad V']$ are linearly independent over $\mathbb{F}_p$, which can be shown to be possible for all $p > 2$. Thus, sum rate of $\frac{3}{2}$ is achieved for structure H in Fig. 19, with channels over $\mathbb{F}_{p^n}$ for all even n, if $\bar{h}_{11} \notin \mathbb{F}_p$. The outer bound of $\frac{3}{2}$ follows from the pair-wise bounds. If all

non-zero channels are equal to 1, then the argument of [31] shows that one destination can decode all messages, i.e., $C = C_{linear} = 1$. In all other cases with non-zero $\bar{h}_{11} \in \mathbb{F}_p$, the linear capacity is still one because the linear capacity is not affected by a scaling of channel coefficients by non-zero constants in $\mathbb{F}_p$. Thus structure I has linear-scheme capacity of $\frac{3}{2}$ if $\bar{h}_{11} \notin \mathbb{F}_p$, and 1 otherwise.

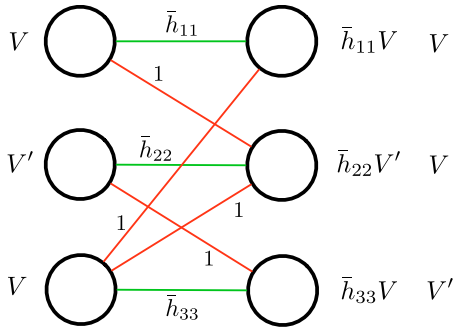

Figure 19: Normalized channel - structure I

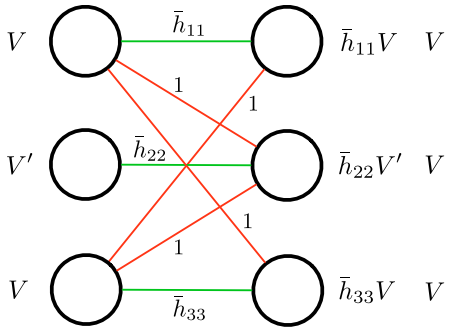

Figure 20: Normalized channel - structure J

Structure J:
The normalized channel for this structure is illustrated in Fig. 20. For this structure, signals from sources 1 and 3 need to be aligned at destination 2 but remain resolvable at destinations 1 and 3. Following the proof for structure D, this can be done if $\bar{h}_{11}, \bar{h}_{33} \notin \mathbb{F}_p$. We choose V such that both $S_1 = [\bar{h}_{11}V \quad V]$ and $S_3 = [\bar{h}_{33}V \quad V]$ are linearly independent over $\mathbb{F}_p$, which can be shown to be possible for all $p > 2$. Thus, sum rate of $\frac{3}{2}$ is achieved for structure J in Fig. 20, with channels over $\mathbb{F}_{p^n}$ for all even n, if $\bar{h}_{11}, \bar{h}_{33} \notin \mathbb{F}_p$. The outer bound of $\frac{3}{2}$ follows from the pair-wise bounds. If all non-zero channels are equal to 1, then the argument of [31] shows that one destination can decode all messages, i.e., $C = C_{linear} = 1$. In all other cases with non-zero $\bar{h}_{kk} \in \mathbb{F}_p$ for any $k = 1, 3$, the linear capacity is still one because the linear capacity is not affected by a scaling of channel coefficients by non-zero constants in $\mathbb{F}_p$. Thus structure J has linear-scheme capacity of $\frac{3}{2}$ if $\bar{h}_{kk} \notin \mathbb{F}_p, k \in \{1, 3\}$, and 1 otherwise.

Finally, let us now consider the setting where only one cross channel is zero.

Structure K:
The normalized channel for this structure is illustrated in Fig. 21. For this single channel structure, interference from sources 2 and 3 need to be aligned at destination 1, and interference from sources 1 and 3 need to be aligned at destination 2.

Beam forming matrix V is used at all 3 sources. Signal spaces at 3 destinations are then given by

$$S_1 = [\bar{h}_{11}V \quad V] = [\bar{h}_{11}v_1, \quad \bar{h}_{11}v_2, \quad \ldots, \quad \bar{h}_{11}v_l, \quad v_1, \quad v_2, \quad \ldots, \quad v_l] \tag{202}$$

$$S_2 = [\bar{h}_{22}V \quad V] = [\bar{h}_{22}v_1, \quad \bar{h}_{22}v_2, \quad \ldots, \quad \bar{h}_{22}v_l, \quad v_1, \quad v_2, \quad \ldots, \quad v_l] \tag{203}$$

$$S_3 = [\bar{h}_{33}V \quad V] = [\bar{h}_{33}v_1, \quad \bar{h}_{33}v_2, \quad \ldots, \quad \bar{h}_{33}v_l, \quad v_1, \quad v_2, \quad \ldots, \quad v_l] \tag{204}$$

Let us choose v_1 as 1, then if $\bar{h}_{11}, \bar{h}_{22}, \bar{h}_{33} \notin \mathbb{F}_p$, $[\bar{h}_{11}v_1 \quad v_1]$, $[\bar{h}_{22}v_1 \quad v_1]$ and $[\bar{h}_{33}v_1 \quad v_1]$ are linearly independent over $\mathbb{F}_p$. Now let us construct v_2 such that 4 columns of $S_k, k \in \{1, 2, 3\}$ are linearly

independent.

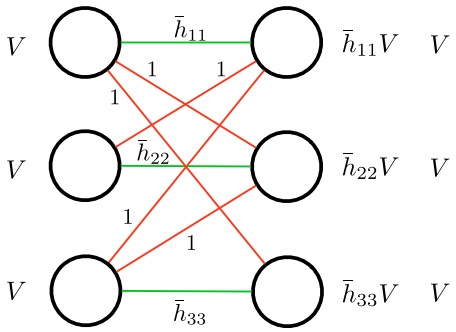

Figure 21: Normalized channel of structure K

$$\text{From } S_k, \quad v_2 \notin A_k \triangleq \left\{ \frac{(\alpha_1 \bar{h}_{kk} + \alpha_2)v_1}{\beta_1 \bar{h}_{kk} + \beta_2} : \alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbb{F}_p, (\beta_1, \beta_2) \neq (0,0) \right\}, k \in \{1,2,3\} \tag{205}$$

Now we note that

$$|A_k| \leq \frac{(p^2-1)p^2}{p-1} = p^3 + p^2 \tag{206}$$

$$|A_1 \cup A_2 \cup A_3| \leq 3(p^3 + p^2) \tag{207}$$

There are p^n choices for v_2, and since $p^n > 3(p^3+p^2)$ for all $p > 3$, there exist choices for v_2 such that all 3 conditions of (205) hold. Choosing v_2 from those, we note that 4 columns of $S_k, k \in \{1,2,3\}$ are linearly independent over $\mathbb{F}_p$. We proceed recursively in a similar manner, for choosing columns $v_3, v_4, \ldots, v_{l-1}$ such that $6, 8, \ldots, 2(l-1)$ columns are linearly independent over $\mathbb{F}_p$ respectively, in $S_k, k \in \{1,2,3\}$.

For the last iteration, we choose column v_l such that all $n = 2l$ columns are linearly independent over $\mathbb{F}_p$ in $S_k, k \in \{1,2,3\}$, given that $2l-2$ columns are already linearly independent with appropriate choices of $v_1, v_2, \ldots, v_{l-1}$.

$$\text{From } S_k, \quad v_l \notin A_k \triangleq \{ \frac{(\alpha_1 \bar{h}_{kk} + \alpha_2)v_1 + (\alpha_3 \bar{h}_{kk} + \alpha_4)v_2 + \cdots + (\alpha_{2l-3} \bar{h}_{kk} + \alpha_{2l-2})v_{l-1}}{\beta_1 \bar{h}_{kk} + \beta_2} : \\ \alpha_i, \beta_1, \beta_2 \in \mathbb{F}_p, i \in \{1, \ldots, 2l-2\}, (\beta_1, \beta_2) \neq (0,0)\}, k \in \{1,2,3\} \tag{208}$$

Now we note that

$$|A_k| \leq \frac{(p^2-1)p^{2l-2}}{p-1} = p^{2l-1} + p^{2l-2} \tag{209}$$

$$|A_1 \cup A_2 \cup A_3| \leq 3(p^{2l-1} + p^{2l-2}) \tag{210}$$

There are $p^n = p^{2l}$ choices for v_l, and since $p^{2l} > 3(p^{2l-1}+p^{2l-2})$ for all $p > 3$, there exist choices for v_l such that conditions of (208) hold. Choosing v_l from those, we note that all n columns of

S_1, S_2, S_3 are linearly independent over $\mathbb{F}_p$.

Hence, desired and interference symbols are linearly independent at all destinations. Thus, sum rate of $\frac{3}{2}$ is achieved for structure K in Fig. 21, with channels over $\mathbb{F}_{p^n}$ for all even n, if $\bar{h}_{11}, \bar{h}_{22}, \bar{h}_{33} \notin \mathbb{F}_p$.

Fraction of channels for which scheme achieves $\frac{3}{2}$ sum rate is given by

$$(\frac{p^n - p}{p^n})^3 = (1 - \frac{1}{p^{n-1}})^3 \to 1 \text{ for large } p, n \tag{211}$$

The outer bound of $\frac{3}{2}$ follows from the pair-wise bounds. If all channels are equal to 1, then the argument of [31] shows that one destination can decode all messages, i.e., $C = C_{linear} = 1$. In all other cases with non-zero $\bar{h}_{kk} \in \mathbb{F}_p$ for any k, the linear capacity is still one because the linear capacity is not affected by a scaling of channel coefficients by non-zero constants in $\mathbb{F}_p$. Thus structure K has linear-scheme capacity of $\frac{3}{2}$ if $\bar{h}_{kk} \notin \mathbb{F}_p, k \in \{1, 2, 3\}$, and 1 otherwise. ■

References

[1] A. Ramakrishnan, A. Das, H. Maleki, A. Markopoulou, S. Jafar, and S. Vishwanath, "Network Coding for Three Unicast Sessions: Interference Alignment Approaches," *Allerton Conference on Communications, Control and Computing*, October 2010.

[2] A. M. S. A. J. Chun Meng, Abinesh Ramakrishnan, "On the feasibility of precoding-based network alignment for three unicast sessions," in *Proceedings of IEEE International Symposium on Information Theory (ISIT), 2012*, pp. 1907–1911, IEEE, 2012.

[3] A. K. Das, S. Vishwanath, S. A. Jafar, and A. Markopoulou, "Network coding for multiple unicasts: An interference alignment approach," *CoRR*, vol. abs/1008.0235, 2010.

[4] V. Cadambe and S. Jafar, "Interference alignment and the degrees of freedom of the K user interference channel," *IEEE Transactions on Information Theory*, vol. 54, pp. 3425–3441, Aug. 2008.

[5] M. Maddah-Ali, A. Motahari, and A. Khandani, "Communication over MIMO X channels: Interference alignment, decomposition, and performance analysis," in *IEEE Trans. on Information Theory*, pp. 3457–3470, August 2008.

[6] S. Jafar and S. Shamai, "Degrees of freedom region for the MIMO X channel," *IEEE Trans. on Information Theory*, vol. 54, pp. 151–170, Jan. 2008.

[7] V. Cadambe, S. Jafar, and C. Wang, "Interference Alignment With Asymmetric Complex Signaling Settling the Høst-Madsen–Nosratinia Conjecture," *IEEE Transactions on Information Theory*, vol. 56, no. 9, pp. 4552–4565, 2010.

[8] A. Motahari, S. Gharan, M. Maddah-Ali, and A. Khandani, "Real interference alignment: Exploiting the potential of single antenna systems," *CoRR*, vol. abs/0908.2282, 2009.

[9] C. Huang, V. Cadambe, and S. Jafar, "Interference alignment and the generalized degrees of freedom of the X channel," *IEEE Transactions on Information Theory*, vol. 58, pp. 5130–5150, August 2012.

[10] U. Niesen and M. A. Maddah-Ali, "Interference alignment: From degrees-of-freedom to constant-gap capacity approximations," *CoRR*, vol. abs/1112.4879, 2011.

[11] V. Cadambe and S. Jafar, "Interference alignment and the degrees of freedom of wireless X networks," *IEEE Trans. on Information Theory*, pp. 3893–3908, Sep 2009.

[12] Z. Wang, "Real interference alignment and degrees of freedom region of wireless X networks," in *International Symposium on Wireless Communication Systems*, 2011.

[13] V. R. Cadambe and S. A. Jafar, "Degrees of freedom of wireless networks with relays, feedback, cooperation and full duplex operation," *IEEE Transactions on Information Theory*, vol. 55, pp. 2334–2344, May 2009.

[14] H. Sun, C. Geng, and S. Jafar, "Degrees of freedom of MIMO X networks: Spatial scale invariance, one-sided decomposability and linear feasibility," *Arxiv preprint ArXiv:11207.6137*, July 2012.

[15] C. Wang, T. Gou, and S. Jafar, "Subspace alignment chains and the degrees of freedom of the three user MIMO interference channel," *Arxiv preprint ArXiv:1109.4350*, September 2011.

[16] C. Wang, T. Gou, and S. Jafar, "Multiple unicast capacity of 2-source 2-sink networks," *CoRR*, vol. abs/1104.0954, 2011.

[17] H. Maleki, V. Cadambe, and S. Jafar, "Index coding – an interference alignment perspective," *ISIT 2012, Preprint of Full Paper available at ArXiv:1205.1483*, 2012.

[18] S. A. J. Sundar R. Krishnamurthy, "Degrees of Freedom of 2-user and 3-user Rank-Deficient MIMO Interference Channels," in *Proceedings of IEEE Global Telecommunications Conference (GLOBECOM), 2012*, IEEE, 2012.

[19] T. Gou and S. Jafar, "Degrees of freedom of the K user M $\times$ N MIMO interference channel," *IEEE Trans. on Information Theory*, vol. 56, pp. 6040–6057, December 2010.

[20] A. Ghasemi, A. Motahari, and A. Khandani, "Interference alignment for the K user MIMO interference channel," in *Proceedings of International Symposium on Information Theory (ISIT)*, pp. 360–364, IEEE, 2010.

[21] H. S. Chenwei Wang and S. A. Jafar, "Genie chains and the Degrees of Freedom of the K-user MIMO Interference Channel," in *IEEE International Symposium on Information Theory(ISIT)*, 2012.

[22] K. Gomadam, V. Cadambe, and S. Jafar, "A distributed numerical approach to interference alignment and applications to wireless interference networks," *IEEE Trans. on Information Theory*, pp. 3309–3322, June 2011.

[23] C. Yetis, T. Gou, S. Jafar, and A. Kayran, "On feasibility of interference alignment in MIMO interference networks," *IEEE Transactions on Signal Processing*, vol. 58, no. 9, pp. 4771–4782, 2010.

[24] G. Bresler, D. Cartwright, and D. Tse, "Settling the feasibility of interference alignment for the MIMO interference channel: the symmetric square case," *CoRR*, vol. abs/1104.0888, 2011.

[25] M. Razaviyayn, G. Lyubeznik, and Z. Luo, "On the degrees of freedom achievable through interference alignment in a MIMO interference channel," *CoRR*, vol. abs/1104.0992, 2011.

[26] I. S. O Gonzalez, C Beltrn, "On the feasibility of interference alignment for the k-user mimo channel with constant coefcients," *ArXiv*, vol. abs/1202.0186, 2012.

[27] M. Z. W. Liangzhong Ruan, Vincent K.N. Lau, "The feasibility conditions for interference alignment in mimo networks," *ArXiv*, vol. abs/1211.3484v1, 2012.

[28] D. C. Guy Bresler and D. Tse, "Geometry of the 3-user mimo interference channel," *ArXiv*, vol. abs/1110.5092, 2011.

[29] G. Bresler and D. Tse, "3 User interference channel: Degrees of freedom as a function of channel diversity," in *47th Annual Allerton Conference on Communication, Control, and Computing*, pp. 265–271, 2009.

[30] T. D. Bavirisetti, G. Abhinav, K. Prasad, and B. S. Rajan, "A transform approach to linear network coding for acyclic networks with delay," *CoRR*, vol. abs/1103.3882, 2011.

[31] V. Cadambe, S. Jafar, "Parallel Gaussian interference channels are not always separable, " *IEEE Transactions on Information Theory*, vol 55, no.9, pp 3983-3990, 2009

[32] R. Etkin, E. Ordentlich, "The Degrees-of-Freedom of the K-User Gaussian Interference Channel Is Discontinuous at Rational Channel Coefficients," *IEEE Trans. on Information Theory*, vol 55, issue 11, pp 4932-4946, Nov 2009.

[33] B. Nazer, M. Gastpar, S. Jafar, S. Vishwanath, "Ergodic Interference Alignment," *IEEE Trans. on Information Theory*, vol 58, no 10, pp 6355-6371, Oct 2012.

[34] Y. Wu, S. Shamai, S. Verdu, "Degrees of Freedom of Interference Channel: a General Formula," *Proceedings of International Symposium on Information Theory (ISIT)* 2011.

[35] S. Jafar, "Interference Alignment: A New Look at Signal Dimensions in a Communication Network," *Foundations and Trends in Communication and Information Theory* pp 1-136, 2011.

[36] R. Lidl, H. Niederreiter, "Introduction to finite fields and their applications", Cambridge University Press, 1986.